24. C. Pomerance and J. W. Smith, *Reduction of huge, sparse matrices over a finite field via created catastrophes*, Experimental Math. **1** (1992), 90-94.
25. O. Schirokauer, *On pro-finite groups and on discrete logarithms*, Ph.D. thesis, University of California, Berkeley, May 1992.
26. D. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inform. Theory **32** (1986), 54-62.

Department of Mathematics
University of Georgia
Athens, Georgia 30602 U.S.A.
e-mail: carl@ada.math.uga.edu

Proceedings of Symposia in Applied Mathematics
Volume 48, 1994

# Factoring Integers Before Computers

H. C. WILLIAMS AND J. O. SHALLIT

*Dedicated to the memory of our friend, D. H. Lehmer* (1905–1991)

ABSTRACT. We examine some aspects of the history of computational number theory, with emphasis on the problems of integer factorization and primality testing.

## 1. Introduction

> *We revel in the details of history because they are the source of our being.*
> *Stephen Jay Gould*

During the last twenty years, the field of computational number theory has achieved the status of a discipline in its own right. This development is due, in large part, to the invention of cryptosystems (methods for encoding and decoding messages) whose security is based on the presumed computational difficulty of certain number-theoretic problems such as integer factorization. Also quite influential was the development of the theory of computational complexity, which enabled the comparison of different algorithms to be placed on a firmer mathematical footing. Because of the influence of these two areas, one may legitimately ask whether computational number theory is properly a part of mathematics or computer science.

But, of course, the most profound influence upon the establishment of computational number theory is the development of the computer. From the very beginning of computer technology (and, as we will see, even before then), number theorists were using whatever "hardware" was available to aid them in their research.

1991 *Mathematics Subject Classification*. Primary 11Y05; Secondary 11Y11, 11A51, 11Y16, 01A55, 01A60.

*Key words and phrases.* Primality testing; factoring.

The research of both authors is supported in part by grants from NSERC of Canada.

This paper is in final form, and no version of it will be submitted for publication elsewhere.

Computational number theory, unlike many other areas of mathematics, is properly a science: experimental method is a significant component in practice. Those who develop number-theoretic algorithms are often concerned with their eventual implementation, and a great deal can be learned from such experimentation.

The release from the immense drudgery of hand calculation afforded by electronic computers leads to a much more thorough development and testing of algorithms, and gives us new insight into the theorems on which those algorithms are based. Furthermore, it becomes possible to use algorithms that are extremely complicated: many powerful modern methods would be completely unusable if only hand computation were available.

Given this, why should we even consider computational number theory before the age of electronic computers? The answer is that the subject was studied for centuries before computers were available, and it is in this work that the modern subject claims its origins. It is important to understand and appreciate the ingenuity and tireless energy of the pioneers of our discipline. It is easy to be condescending toward these people; after all, they did not express their ideas using modern terms such as "polynomial time" or "succinct certificate" that we casually use today. Although they had not formulated such language, they often understood the ideas implicitly.[1] Since they did their calculations by hand or with the aid of simple mechanical tools, they had to be concerned with efficiency and accuracy.

Why did the early workers in computational number theory not use machines? The answer is that they did: not only did they make use of whatever calculating device was available at the time, on occasion they even developed new machines, as we will see later. One great difficulty that frequently plagued these researchers was that the technology of the day was simply not equal to the demands of the mechanisms they envisaged. For example, according to some historians, Babbage's failures with the differential engine were due in part to the inadequacy of the British machine-tool industry at the time (but for a different view, see [**176**]). A sieving device described by Lawrence in 1896 was only constructed successfully by Carissan in 1919. Furthermore, it was not until 1932 that Lehmer was able to make a sieve mechanism run at a fairly rapid rate without human intervention. Another problem, easy to appreciate by researchers of today, was the difficulty in obtaining research funding for these projects.

We do not intend in this paper to provide anything like a complete history of the development of computational number theory. For our purposes, it will suffice to illustrate our points by concentrating on one particular problem which is still of great interest today: the integer factoring problem. Indeed, the only "proof" that this problem is intractible (a very important issue in modern cryptography) is based on its history. More precisely, we will study the computational history of both factoring and primality testing. These two problems really do belong together, because if we wish to obtain the complete factorization of an integer $N$ as a product of prime powers, we must be able to show that the primes involved in this representation are indeed primes. Also, as we will see below, a partial factorization of numbers like $N-1$ and $N+1$ proves useful if one wants to prove that $N$ is prime.

These problems have a very long history, but, with the exception of the invention of the Eratosthenian sieve, nothing truly significant was done until the time of Fermat. From then on, progress has been steady (if not always spectacular) up to the present day.

We emphasize here that early researchers in computational number theory were often uninterested in general methods for factorization or primality testing; rather, particular classes of numbers (such as $2^n \pm 1$ and $10^n \pm 1$) served as stimuli for their efforts. The reader is no doubt familiar with the stories of Mersenne's discussion of the primality of $2^n - 1$, and Fermat's incorrect belief that all numbers of the form $2^{2^n}+1$ are prime. In 1856, Reuschle [**159**] published (among other items) a table of factors of $2^n - 1$ and $10^n - 1$ for $n \leq 42$, and in 1869, Landry [**63**] published a table of factors of $2^n \pm 1$ for $n \leq 64$. The "holes" in these and other tables provided a source of challenges in factoring and primality testing that occupied the energies of many workers over several decades, as do the holes in the Cunningham Table [**13**] even today.

Our main focus in this paper is on the computational history of factoring and primality testing from 1750 to about 1950 (although we discuss modern work in §14). (For citations before 1750, the reader may consult Volume 1 of Dickson's History of the Theory of Numbers [**20**].) Nevertheless, it may be of some interest for comparison's sake to mention what can currently be done. The largest prime currently known is $2^{756839} - 1$, a number of 227832 decimal digits. This was discovered by Slowinski and Gage on 19 February 1992; see Ewing [**23**]. One of the largest integers ever proved prime by a general method[2] is $(2^{3539}+1)/3$, a number with 1065 decimal digits; see Atkin and Morain [**3**] and Bosma and van der Hulst [**10**]. D. Bernstein and A. K. Lenstra announced the factorization of $2^{523} - 1$, a 158-digit number, on 29 October 1992; they used the lattice sieve, a version of the number-field sieve. The largest integer ever factored by a general method is a 116-digit divisor of $10^{142}+1$, by A. K. Lenstra, M. Manasse, and the assistance of many others; see [**98**]. For further information on this subject, we refer the reader to the papers of Williams [**186**], Silverman [**172**], and the books of Riesel [**161**], Bressoud [**11**], and the Cunningham project book of Brillhart et al. [**13**].

[1] In making this observation, we hope, of course, to avoid the fallacy of interpreting historical events solely in the light of modern understanding.

[2] By a *general method* we understand an algorithm that does not depend on any special properties of its input. For example, a primality testing algorithm that applies only to numbers of the form $2^n - 1$ would not be a general method.

## 2. Primality testing

We begin our discussion of the history of computational number theory with the problem of testing a positive integer for primality.

From a modern point of view, the definition of the term "primality test" is not universally agreed upon. (Indeed, the authors of this paper are not in complete agreement!) In general usage, a *test* can mean a "procedure for determining the presence or absence of some property"; consider, for example, "syphilis test". As the term is generally understood, a test may not be accurate with 100% confidence. It is also possible for a test to return the result "inconclusive".

This intuitive usage of the term "test" is what is generally meant by most complexity theorists. By a "primality test", most complexity theorists understand any randomized algorithm[3] that recognizes either the set of prime numbers or the set of composite numbers. More precisely, any Atlantic City algorithm is regarded as satisfactory; here, Atlantic City refers to an algorithm with the property that the output may be incorrect, but the probability of error is no more than $1/2 - \epsilon$, for some fixed positive constant $\epsilon$. It is important to note that the probability of error does not depend on the input $N$; rather it is computed by considering all possible sequences of coin flips used by the algorithm. If a set is accepted by an Atlantic City algorithm running in polynomial time, then we say that the set is in the complexity class BPP (bounded away from zero probabilistic polynomial time). It is known that the set of prime numbers are in this class; thus, complexity theorists and cryptographers are generally happy with the algorithms of Solovay-Strassen [**173**] and Miller-Rabin [**156**].

However, many number theorists find this rather general definition unsatisfactory, since Atlantic City primality tests do not, in general, provide a proof that a prime number really is prime - only good evidence that this is the case. (However, the Solovay-Strassen and Miller-Rabin algorithms actually have one-sided error, and hence if they reply "composite" on input $N$, then a proof that $N$ is composite is provided by the details of the computation.) In contrast, most number theorists do not object on philosophical grounds to the so-called Las Vegas tests: these use a source of random numbers, but their output does provide a proof that the number in question is either prime or composite. Only the running time, not the conclusion, of a Las Vegas algorithm is probabilistic. If a set is accepted by a Las Vegas algorithm running in expected polynomial time, then we say that the set is in the complexity class ZPP (zero error probabilistic polynomial time).

As most of the early workers tended to regard a primality test as being a technique which would yield a rigorous proof of primality, we will adopt for use throughout this paper the following more narrow definition of "primality test":

DEFINITION 2.1. A primality test on a given integer $N$ is the computational verification of the hypothesis of a theorem whose conclusion is that $N$ is prime.

Some have also called such a test a "primality proof".

Many such tests can be described. For example, consider Wilson's theorem (which was probably known to Leibniz; see Vacca [**185**] and Mahnke [**127**]): $N > 1$ is a prime if and only if $N$ divides $(N-1)! + 1$. However, this test seems to be computationally impractical, since there is no known way to compute $(N-1)! + 1 \pmod{N}$ in any reasonable length of time for large $N$. (Note that Wilson's Theorem actually gives a necessary and sufficient test for primality, something not explicitly required by our definition.)

Having described what we mean by a primality test, we now give four features that are desirable: the test should be efficient, the test should be universally applicable, the test should be robust, and the test should produce an efficiently verifiable certificate of primality.

The term "efficient" is, of course rather vague and subject to interpretation, but most would agree that the obvious implementation of Wilson's theorem is not efficient. Today we might say that an algorithm is efficient if it runs in polynomial time, that is, if its running time is bounded by a polynomial in $\log N$, where $N$ is the input. This definition has its problems in real life, however, since the polynomial referred to may have high degree or very large coefficients. For example, although it is a great theoretical advance, the Las Vegas primality test of Adleman and Huang [**1**] is probably not useful in practice for precisely these reasons.

The second feature, universal applicability, means that the test should work for all prime numbers. This is a desirable goal, but one that not all otherwise useful tests satisfy. As we will see below, many of the early practical primality tests only worked for numbers of special forms: Lucas' test for numbers of the form $2^p - 1$, for example.

The third desirable feature of a primality test is robustness. Robustness is a vague notion which is difficult to express precisely; we use it to mean that errors that take place during the course of the computation will be detectable. Here is an example: suppose we are trying to determine if a number $a$ is a quadratic residue modulo some given odd prime $p$. By Euler's criterion, it suffices to compute $a^{(p-1)/2} \pmod{p}$. The result, if computed correctly, will be $+1$ or $-1$, according to whether $a$ is a residue or nonresidue. Nearly every mistake made in this computation will be detectable, since most will result in an answer which is neither $+1$ nor $-1$.

Robustness was especially important in the days before computers, when hand computation was very error-prone, and checking a computation was not simply a matter of running a program again on another machine. Lucas' necessary and sufficient test for primality of numbers of the form $2^p - 1$ depends on obtaining the result 0 after a long series of hand calculations involving numbers with $p$ bits. If the result is 0, then one may be reasonably confident that it is correct, and hence the number in question is prime, since the probability of obtaining 0

[3] A *randomized algorithm* is one that has access to a sequence of random, unbiased flips of a fair coin.

after a random series of multiplications and additions of numbers this large is quite small. On the other hand, if the result is not 0, the theory implies that the number in question is composite. But since almost any error introduced into the computation would also give a nonzero result, one's confidence in this result is necessarily smaller.

The last criterion, that of producing an easily verifiable certificate of primality, was explicitly pointed out for the first time by Pratt in 1975 [**150**]. He showed that, for any given prime $p$, it is possible to obtain a "succinct certificate" that proves $p$ prime and which can be verified in polynomial time. It is, of course, quite conceivable that actually *finding* such a certificate may require more than polynomial time.

Note that we have not discussed what may happen if the input to a primality test is composite. There are several possibilities: the algorithm may diverge (run forever); the algorithm may reply that the test is inconclusive; or the algorithm may provide a proof that the input is indeed composite. While this behaviour was a legitimate concern in the past, today a proof of compositeness may be given in polynomial expected time using the strong pseudoprime test (as in Miller-Rabin).

Having discussed some abstract principles, we now move on to the history of primality testing. In 1588, Cataldi proved that $N_1 = 524287 = 2^{19} - 1$ is a prime by trial division by all the primes less than the square root of $N_1$. (The method of trial division was known to Fibonacci in 1202.) Until 1772, this seems to have been the largest prime known. At that time, Euler proved that $N_2 = 2147483647 = 2^{31} - 1$ is a prime. He did this by improving upon the algorithm used by Cataldi.

Euler was aware that if any prime $q$ is a divisor of $2^p - 1$, where $p$ is an odd prime, then $q \equiv 1 \pmod{2p}$, a result known to Fermat. He also realized that since $2N_2 = (2^{16})^2 - 2$, then 2 must be a quadratic residue of $q$; hence $q \equiv \pm 1 \pmod 8$. By combining these observations, Euler could assert that if $q$ is a prime divisor of $N_2$, then $q = 248k + 1$ or $q = 248k + 63$ for some integer $k \geq 0$. If $q < \sqrt{N_2}$, then there are only at most 186 values of $k$ to check. Thus, after performing at most 372 trial divisions (fewer if one eliminates composite trial values of $q$), Euler was able to show that $N_2$ is a prime. Thus, Euler's test was more efficient than Cataldi's.

In 1859, F. Landry [**61**], who at that time believed that $2^{31} - 1$ was still the largest known prime[4], attempted to give a shorter proof of its primality than Euler's. By using a number of clever tricks he was able to do this; in fact, by 1867 he was able to claim [**62**] that he had so reduced the calculations necessary to effect the verification of the primality of $N_2$ that they would fit on a single slip of paper. Furthermore, in this same paper Landry goes on to state that he had proved the primality of the thirteen-digit divisor 1133836730401 of $2^{75} + 1$.

[4] In fact, according to Reuschle [**159**, p. 3], Looff had proved in 1851 that 999999000001, the 12-digit factor of $10^{18} + 1$, is prime.

What he said next we quote here, in translation from the French:

> At this point we are, if not uneasy, then at least somewhat embarrassed.
>
> Indeed, when one has succeeded in factoring a number, and has given its factors, this can be verified immediately. But it is a different matter when the methods used fail to discover any factor, and one then asserts that the number is prime. How could one then transmit to another such a totally personal conviction? Who would be convinced, without having redone all the calculations, and without having understood the principles on which those calculations were based?
>
> We understand well that our claim is valid only as an assertion, worthwhile until someone proves the contrary, or until we make known our methods and enable others to apply them.

Today, we would say that Landry was struggling with the difficulty of providing a *succinct certificate*. Landry clearly anticipated the basic idea of what would become famous a hundred years later in computational complexity theory: the class NP. Even today, providing such a certificate is a difficult problem, and those who have been involved in primality testing can easily understand and appreciate Landry's concern.

In 1869, Landry [**63**] went on to state that he had proved that the 14-digit number $(2^{53} + 1)/(3 \cdot 107)$ is prime. This was the largest prime known until 1876, when Lucas made his breakthrough. Incidentally, Landry did not describe in [**62, 63**] how he had carried out his impressive factorizations. It was not until 1880, when he wrote a letter [**64**] to Charles Henry, that he revealed his method. Landry's technique had been known to Fermat and will be described later. (It was this convergence of techniques that particularly struck Landry and caused him to write his letter.) After Landry's work in 1869, only the following four numbers of the form $2^n \pm 1$ ($n \leq 64$) remained unfactored:

$$2^{59} - 1, 2^{61} - 1, 2^{61} + 1, 2^{64} + 1.$$

By 1878, Landry (according to Lucas [**114**, pp. 239–240]) had factored $2^{59} - 1$; we will discuss the investigation of the others later. It is interesting to note in passing that Landry suspected that $2^{61} - 1, (2^{61} + 1)/3$, and $2^{64} + 1$ were all primes, but he never seems to have said that he had proved the primality of any of them. Indeed, in [**63**] he stated that these had resisted his efforts, and in 1880 he said [**64**] that the first two still remain to be investigated (the third is composite).

**2.1. Babbage.** Charles Babbage, the English pioneer of the modern computer, was one of the first to apply computational ideas to number theory.

Legendre and Euler had both noticed that the polynomials $x^2 \pm x + 41$ had the unusual property of generating nothing but primes for small values of $x$. The relationship between this curiosity and the class number of $\mathbb{Q}(\sqrt{-163})$ was not explained until 1912 by Frobenius and Rabinovitch. Babbage knew about these polynomials, and one of the first tasks he set his Difference Engine to was the computation of values of $x^2 + x + 41$. In June 1822, he wrote:

> With this machine I have constructed ... a table from the singular formula $x^2 + x + 41$, which comprises amongst its terms so many prime numbers.

His machine could only display results, and not print them. Babbage employed a friend to write down the results. In a letter to Sir Humphrey Davy the next month, Babbage discussed the speed of his machine:

> [The Difference Engine] proceeded to make a table from the formula $x^2+x+41$. In the earlier numbers my friend, in writing quickly, rather more than kept pace with the engine; but as soon as four figures were required, the machine was at least equal in speed to the writer.

The letter also mentioned a possibility for a future machine (perhaps the Analytical Engine):

> I have also certain principles by which, if it should be desirable, a table of prime numbers might be made, extending from 0 to ten millions.

See Babbage's collected letters and papers [**4**] for more details.

## 3. Lucas' discovery

In order to discuss the work of Edouard Lucas, it is first necessary to introduce the functions that today carry his name. The Lucas functions $U_n$ and $V_n$ (or $U_n(P,Q)$ and $V_n(P,Q)$) are defined by

$$U_n = U_n(P,Q) = (\alpha^n - \beta^n)/(\alpha - \beta),$$

$$V_n = V_n(P,Q) = \alpha^n + \beta^n,$$

where $\alpha, \beta$ are the zeros of the polynomial $x^2 - Px + Q$, and $P, Q$ are coprime integers.

These functions did not originate with Lucas; they (or functions very similar to them) had been studied by Euler, Lagrange, Legendre, and Gauss. Several combinatorial and number-theoretic properties of the function $U_n$ had been discovered by Siebeck [**171**] almost thirty years previous to Lucas' work. Also, Genocchi [**33**] had used properties of functions very similar to $U_n$ and $V_n$ in order to demonstrate the infinitude of primes of the forms $ax + 1$ and $ax - 1$, for any given $a$. Nevertheless, in our opinion the functions are properly called the Lucas functions because of Lucas' singular contribution to their study, only a part of which we will discuss here.

In early January of 1876, it appears that Lucas [**102**] had considered the functions $U_n$ and $V_n$ as we see them above, but he was mainly interested in the particular case of $U_n(P,Q)$ where $P = 1$ and $Q = -1$. Today, these numbers are called Fibonacci numbers, but at the time it was common to call the sequence

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots \tag{3.1}$$

the series of Lamé. That was because Lamé [**60**] in 1844 had used these numbers to investigate the number of steps performed by the Euclidean algorithm to compute the greatest common divisor of two numbers. Lamé had shown that the worst case of the Euclidean algorithm occurred when the inputs were successive Fibonacci numbers, a fact that had been given without proof by Léger [**69**] in 1837. This is one of the earliest results in the analysis of algorithms. Lamé further showed that the number of division steps in the Euclidean algorithm was always bounded by five times the number of decimal digits in the smaller of the two inputs. It was Lucas, however (see [**103**] and [**112**]), who discovered that these numbers had been known to Fibonacci six centuries earlier, and in Lucas' next paper [**103**] dated May of 1876, he calls (3.1) the Fibonacci series.

There are several results mentioned in [**102**], all given without proof, but the most striking of these are results such as the following.

THEOREM 3.1. *If $N \equiv \pm 3 \pmod{10}$, $N | U_{N+1}$, and $N \nmid U_d$ for all divisors $d$ of $N+1$ [with $d < N+1$], then $N$ is a prime.*

The reason for the importance of this theorem will be fully discussed later. Lucas pointed out that it permits one to know that a number is prime or composite without the need of a table of primes, i.e., without employing trial division. Notice that this is somewhat similar in spirit to Wilson's theorem in that to show that $N$ is a prime it is necessary to show that it divides a certain number. However, Lucas was the first individual to devise an efficient test for primality or compositeness, which did not necessarily have to reveal the factors, if any, of the number being tested. He then goes on to say:

> It is with the aid of this theorem that I think that I have shown that the number $N = 2^{127} - 1$ is a prime.

This $N = 170141183460469231731687303715884105727$ is a number of 39 digits, far greater than the largest prime known at the time. (Lucas at this time was unaware of the work of Looff and Landry and thought that $2^{31} - 1$ was the largest known prime.)

Lucas had clearly made a most remarkable discovery, and when we think about his statement today, there are at least four important questions that we are led to ask:

(i) *How* did Lucas discover this test?
(ii) *Why* did he test $2^{127} - 1$, and not some other number?
(iii) *How* did he test $2^{127} - 1$?
(iv) *Why* was he unsure of the result?

We will attempt to answer the first two of these questions in this section, leaving for later sections the answers to the others. Previous to his paper [**102**], Lucas had written only one other paper [**101**] on factoring. In this paper he attempts to factor various numbers of the form $a^n \pm 1$ by determining the possible linear forms of the prime divisors (as did Euler) and then performing trial divisions by taking logarithms of the numbers involved and subtracting. This work, which appeared in November of 1875, seems much less sophisticated than the work of the following January. What happened? In [**118**, p. 14] Lucas himself provides us with the answer. In commenting on [**102**] he says:

> This note is the point of departure for new investigations by the author in the theory of prime numbers. After having decomposed by means of a table of prime divisors the early terms [of the Fibonacci numbers], the observations of the forms of these divisors led the author to the demonstration of a certain number of theorems which allowed him to develop some new and general considerations concerning the theory of prime numbers. One finds here for the first time an indication of a new method for finding prime numbers, which is independent of a previously constructed table of prime numbers.

As to why Lucas selected $2^{127}-1$ to test, we can only speculate. Probably he wanted to find a prime of the form $M_n = 2^n - 1$; after all, Euler himself had been interested in such primes and Euclid had shown that $2^{n-1}M_n$ is a perfect number when $M_n$ is a prime. Also, it is easy to find all of the divisors of $M_n + 1 = 2^n$; thus, the theorem of Lucas quoted earlier is easy to apply (see §4 below). Lucas knew that any prime value of $M_n$ would require that $n$ be prime and he also knew all the primes of the form $M_n$ that had been identified by 1876:

$$2^2-1, 2^3-1, 2^5-1, 2^7-1, 2^{13}-1, 2^{17}-1, 2^{19}-1, 2^{31}-1.$$

Notice that some of these values of $n$ (i.e., 3, 7, 31) are also of the form $M_k$. The next possible prime value for such an $n$ is 127 and $M_{127} \equiv -3 \pmod{10}$; thus, his theorem could be used. We don't really know that this was how Lucas was thinking, but in a later letter [**111**] he speculates on the existence of a sequence of primes of the form $2^n-1, 2^{n_1}-1, 2^{n_2}-1, \ldots$, where $n_1 = 2^n - 1$, $n_2 = 2^{n_1} - 1$, etc.; thus, it's quite likely that he was thinking along the lines of our speculation. According to [**118**], Lucas wrote a thesis for presentation to the Faculty of Science at Paris. This thesis, dated September 24, 1877, was a development of the paper [**102**] and could perhaps cast some further light on these problems. Unfortunately, all attempts by the authors to locate a copy of it have so far failed.

## 4. Implementation of Lucas' test

In order to discuss how Lucas actually used his theorem to test $M_{127}$, we provide the following simple identities satisfied by $U_n$ and $V_n$:

$$U_{2n} = U_n V_n;$$

$$V_{2n} = V_n^2 - 2Q_n.$$

On examining these identities and referring back to Lucas' theorem, it is easy to see that if $N = 2^n - 1$ and $N|U_{N+1}$ but $N\nmid U_d$ for any proper divisor $d$ of $N+1$, then $N|V_{(N+1)/2}$. Thus, if we define $S_k = V_{2^k}(1,-1)$, then $S_k = S_{k-1}^2 - 2$ for $k \geq 2$. We have the following test:

If $M_n \equiv \pm 3 \pmod{10}$, then $M_n$ is a prime if $M_n|S_{n-1}$, where $S_1 = 3$ and $S_k \equiv S_{k-1}^2 - 2 \pmod{M_n}$ $(k = 2, 3, ..., n-1)$.

Notice that this test for primality certainly possesses the features of efficiency and robustness discussed in §2. As he mentions in [**112**], this is the form of the test that Lucas used. By December of 1876 he [**107**] has modified this result as follows:

THEOREM 4.1. *Let $p = 2^{4m+3} - 1$, where the exponent is a prime. If one forms the sequence*

$$3, 7, 47, 2207, \ldots$$

*with $r_1 = 3$ and $r_{n+1} = r_n^2 - 2$, then $p$ is a prime when the least value of $k$ such that $p|r_k$ is $4m+2$. The number is composite if none of the first $4m+2$ values of $r_n$ is divisible by $p$. Finally, if $\alpha$ denotes the first value of $k$ such that $p|r_k$, then the [prime] divisors of $p$ have the form $2^\alpha t \pm 1$ combined with those forms which can divide $x^2 - 2y^2$.*

So we know what sort of test Lucas used, but how did he actually perform the arithmetic? Remember $M_{127}$ is a number of 39 digits; the kind of arithmetic needed here would involve numbers larger than any used previously. In several papers Lucas [**103, 106, 108, 114**] alludes to the use of binary arithmetic for doing this, but he does not really describe how he actually did it. Finally, in [**112**, p. 152 ff] he is more explicit. The solution to this problem is very characteristic of him; he made the performance of this tedious arithmetic into something like a game. He said he used a 127 × 127 chessboard to effect the computations. To illustrate his idea he used a simple example which we will discuss here.

Consider (instead of $M_{127}$) $M_7 = 2^7 - 1 = 127$. We have $S_1 = 3$, $S_2 = 7$, $S_3 = 47$, $S_4 = 472 - 2 \equiv 48 \pmod{127}$, $S_5 \equiv 482 - 2 \equiv 16 \pmod{127}$, $S_6 \equiv 162 - 2 \equiv 0 \pmod{127}$; hence, we have a proof of the primality of 127. Lucas notes that if $M_n = 2^n - 1$, then

$$2^{n+m} \equiv 2^m \pmod{M_n}. \tag{4.1}$$

The main operation of testing involves squaring, subtracting 2, and reduction modulo $M_n$. If we try to perform this on $S_3$ to obtain $S_4$ (using $M_7$) we first consider the binary representation of $S_3$ which is 101111. We can then begin to compute its square by simply multiplying as usual

$$\begin{array}{ccccccccccc}
 & & & & & 1 & 0 & 1 & 1 & 1 & 1 \\
 & & & & & 1 & 0 & 1 & 1 & 1 & 1 \\
\hline
 & & & & & 1 & 0 & 1 & 1 & 1 & 1 \\
 & & & & 1 & 0 & 1 & 1 & 1 & 1 & \\
 & & & 1 & 0 & 1 & 1 & 1 & 1 & & \\
 & & 1 & 0 & 1 & 1 & 1 & 1 & & & \\
 & 0 & 0 & 0 & 0 & 0 & 0 & & & & \\
1 & 0 & 1 & 1 & 1 & 1 & & & & & \\
\hline
\end{array}$$

However, because we only need to find the answer modulo $2^7 - 1$, we can use (4.1) to put the information between the horizontal lines into a neat $7 \times 7$ square because each row wraps around cyclically.

| 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 1 | 1 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 0 | 1 | 1 | 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 1 | 0 | 1 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 0 | 1 | 0 | 1 | 1 |

In order to avoid a lot of writing, Lucas suggests the use of a $7 \times 7$ chessboard with pawns in squares representing the positions of the ones and empty squares representing the positions of the zeros.

Once we have this array of pawns on our chessboard we make use of two rules:

(i) Take (when possible but only once) a pawn away from column 2. This corresponds to the subtraction of 2 from the square. If a pawn never appears in column 2, then 2 must be subtracted from the final answer.

(ii) For each pair of pawns in any column remove one from the board and move the other into the column to the left. Remember that the column to the left of the left-most column (column 7 here) is column 1 because of (4.1).

Continue performing these operations until the only pawns remaining are in the first row. In our case we get the first row to be

| 7 | 6 | 5 | 4 | 3 | 2 | 1 |
|---|---|---|---|---|---|---|
|  | ● | ● |  |  |  |  |

which represents 0 1 1 0 0 0 0 or 48 in decimal.

Lucas said that with a little training one can succeed in becoming quite quick at the manoeuvre (ii) above. By making use of a $127 \times 127$ chessboard, this was how Lucas performed his test on $M_{127}$. The advantage of not having to write anything down (contrary to Lehmer's criticism in [**71**]) is to some degree offset by having nothing left at the end of the process but an answer. If an error were made, it would be difficult to detect. Depending on how quickly Lucas could execute the operations needed to perform this test, we estimate that it must have taken between 170–300 hours for him to complete it. This explains why he only performed this test of $M_{127}$ a single time (see [**112**, p. 152]), and this may be why he was a little unsure of his result, but we'll discuss this more fully in §5.

One thing that is very striking about Lucas' technique is how easy it should be to mechanize (and how much more accurate the results would be if it were). Certainly, Lucas thought so. In several of his papers [**103, 105, 106, 107**]; and [**114**, p. 305] he mentions the possibility of constructing a machine for doing this. For example in [**103**] he says:

> The construction of this mechanism allows for the rapid calculation in the binary number system of residues of the $V_n$ with respect to the number whose decomposition we are seeking. It is based on the preceding theorems and the mathematical laws of the geometry of weaving.

In [**106**] he goes so far as to say:

> I have conceived ... the plan of a mechanism which allows ... for the determination of prime numbers having a thousand digits in the decimal system.

The reference to the geometry of weaving is not as outlandish as it may seem. Lucas knew a great deal about weaving and wrote or presented several papers on this subject. Also, there were mechanisms in existence at that time which did allow for the construction of a fabric with the properties of the chessboard representation of the square of an integer (mod $M_n$) discussed above. In this representation a 1 might be denoted by a vertical thread passing over a horizontal one, whereas a zero would then be represented by a vertical thread passing under a horizontal one. Nevertheless, by the time Lucas published in 1878 his main work [**114**] on the Lucas Functions, his claims are much more subdued. Also, in his major paper on the geometry of weaving [**119**] (see [**126**] for a French translation) he makes no mention of using his ideas for constructing a machine. However, he never forgot these ideas, and in 1887 he says [**121**]:

> I will add that Mr. Genaille is currently constructing for me a machine that will enable us to [find all primes of the form $2^n - 1$] which have no more than 150 digits.

Henri Genaille was a very prolific inventor of calculating mechanisms. Lucas praises him very warmly in his paper on calculating devices, which was reprinted in Vol. III of *Récréations* [**125**]. He is credited with constructing over 28 such devices in [**129**], all of which were donated in 1886–1888 to the Conservatoire National des Arts et Métiers in Paris. Also, he and Lucas worked together on a number of various computing devices (see [**2**]), and in 1891 we learn in an all-too-brief mention [**32**] that he had constructed an Arithmetic Piano, a device which was to be used for determining primes of the form $2^n - 1$. We quote the article [**32**] in full:

> The Arithmetic piano allows one to put into practice the method formulated by Mr. E. Lucas, at the Congress of Clermont-Ferrand, for the verification of large prime numbers. By the simple manoeuvering of some pegs, the verification of prime numbers of the form $2^n - 1$ is reduced in the greater number of cases to a labour of a few hours. This machine, which can manage to carry out automatically calculations of the greatest importance, will effect one day the realization of a calculating machine which performs arithmetic operations by itself.

We have currently no idea what happened to this machine. Unfortunately, Lucas died at the early age of 49 a few weeks after the meeting at which the machine was exhibited and nothing seems to have been heard about it since.

Gérardin [**40**], writing in 1912, claimed that Genaille had not constructed anything, but this is certainly not the sense of [**31**], where it is explicitly stated that the machine was admired by all the members of the session. Indeed, in view of the facts that 1) Genaille was a skilled fabricator of calculation machines and 2) that he had been working on this device for a period of about 4 years, it is difficult to believe that he would have discussed a nonexistent mechanism. However, it is possible that the device was not in a completely finished state. Very likely the machine was in the possession of Genaille when Lucas died, and there being no further use for it, Genaille probably abandoned the project. We wonder if somewhere in France this machine might still exist.

It is curious to note that both Fauquembergue [**25**] in 1912 and Mason [**128**] in 1914 described devices based on Lucas' ideas for testing the primality of $M_n$, devices which were based on the same multiplication technique of Cauchy [**18**], even though it appears that Mason was unaware of [**18**]. In the case of Fauquembergue, a device resembling a rather large slide rule was actually constructed and used. Mason's device, which was more sophisticated in concept than that of Fauquembergue, seems never to have been constructed.

## 5. Lucas and Mersenne

The most difficult-to-answer of all the questions posed in §3 is (iv). This is because it does not appear that Lucas had ever settled this question in his own mind. What is particularly remarkable is his failure to mention the primality of $M_{127}$ in several of his papers where it would have been appropriate, especially in his memoir [**114**], the notice of his works [**118**], or his book [**122**]. In many ways his doubts or caveats, expressed in one way or another in [**102, 112, 120, 121, 123, 124**] seem strange to us today. For, after going through all the labour necessary to find $S_{126} \pmod{M_{127}}$ and finding it to be the particular residue zero, and considering all the possibilities for error, he would almost certainly have had the correct answer. The probability that it would be wrong is very remote indeed. However, this is not necessarily the way that Lucas thought about these matters. Remember that he had just discovered this test and did not have all the experience in these matters that we have today.

He was evidently of two minds concerning his result; nowhere is this better illustrated than in his paper [**120**], written in 1886. This note seems to have been in response to one of Seelhoff [**165**] (see also [**164**]) in which, among other matters, it was stated that there were only eight perfect numbers known. Lucas replied that there were *nine* (his italics) such numbers and listed $2^{126}M_{127}$ as one. Since from the time of Euler, it has been known that the only even perfect numbers are those of the form $2^{n-1}M_n$, where $M_n$ is a prime, it is clear at this point that Lucas considered $M_{127}$ a prime. However, on the next page of this same note he gave a list of 24 values of $n$ up to 257 which includes the number 127. Of this list of values he stated that it remains to study (meaning in this context to determine the prime or composite character of) the values of $2^n - 1$, for these $n$-values, a statement he also made in [**122**, p. 376].

The likely cause of Lucas' difficulties was a statement of Mersenne. In 1644, Mersenne asserted (without giving any reason) that of the 55 prime values of $n \leq 257$, $M_n$ is a prime for only the following 11 values:

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

Mersenne was a correspondent of many of the great mathematical thinkers of his time such as Descartes, Fermat, and Frenicle; thus, this statement carried a lot of weight. The attentive reader might well ask why it was not this list that caused Lucas to attempt to prove $M_{127}$ a prime? (The symbol $M$ here commemorates Mersenne and numbers of the form $M_n$, where $n$ is a prime, are called Mersenne numbers today.) The answer to that question is that Lucas was unaware of Mersenne's list when he tested $M_{127}$. He was informed of it later in a paper [**34**] of Genocchi, where the list is mentioned in a lengthy footnote.

While it is hard for us to understand this today, it is important to realize that throughout most of his academic life, Lucas attached considerable importance to Mersenne's list. We now know that it contains five errors ($M_{67}$ and $M_{257}$ are composite and $M_{61}$, $M_{89}$, $M_{107}$ are primes). In fact, in [**113**] Lucas declared that Mersenne was in possession of arithmetical methods that are now lost. In [**114**, p. 237] he went on to say that Mersenne's method would probably not deviate from the principles of Fermat, and as a consequence, would not differ essentially from the method he (Lucas) had deduced. Another part of the reason he believed in this list is that until 1887 every factoring result concerning Mersenne numbers, of which Lucas was aware, confirmed the truth of it. Indeed, the 24 values of $n$ mentioned earlier were all that remained to be tested of the original 55. His faith in Mersenne's list was so strong that he seems to have refused to believe the results of his own calculations on $M_{67}$. In [**103**] he states that he does not think that 67 belongs in the list because he had already applied his method to it. But later in [**114**, p. 307] he says:

> One could thus construct diagrams for prime numbers of the form $2^{4q+3}-1\ldots$ we hope ultimately to give these for the numbers $2^{67}-1$ and $2^{127}-1$.

These diagrams were depictions of $n \times n$ chessboards whose rows represented in binary the residues $S_k$ modulo $M_n$ for $k = 0$ ($S_0 = 0$), $1, 2, \ldots, n-1$. For example, the diagram for $M_7$ would appear as

| 6 | 5 | 4 | 3 | 2 | 1 | 0 | |
|---|---|---|---|---|---|---|---|
| | | | | | | ● | 0 |
| | | | | | ● | ● | 1 |
| | | | | ● | ● | ● | 2 |
| | ● | | ● | ● | ● | ● | 3 |
| | ● | ● | | | | | 4 |
| | | ● | | | | | 5 |
| | | | | | | | 6 |

In fact, Lucas [**112**] went to some trouble to compute such a diagram for $M_{31}$. This represented his attempt at producing a succinct certificate for its primality. He [**104**] also issued, as a challenge, the problem of proving $M_{31}$ a prime without the use of a table of primes.

In 1887, Lucas [**121**] learned that $M_{61}$ is a prime. Seelhoff [**168**] had shown this in 1886, and Hudelot, after 54 hours of labour, in 1887 confirmed Seelhoff's result. This confirmation was very much needed, as Seelhoff's proof is certainly not complete. He appears to have done little more than verify that

$$3^{N-1} \equiv 1 \pmod{N}$$

for $N = M_{61}$. This is certainly a necessary condition for primality, but it is not sufficient, as Lucas himself well knew. Hudelot made use of the following test of Lucas [**124**] (see also [**110**]).

THEOREM 5.1. *If $p = 2^{4m+1}-1$, where $4m+1$ is a prime, then $p$ is a prime if $p|S_{4m}$, where $S_1 = 4$ and $S_k \equiv S_{k-1}^2 - 2 \pmod{p}$ $(k = 2, 3, \ldots, 4m)$.*

Hudelot's result is correct, but in fact Pervouchine (see Imchenetzki and Bouniakowsky [**49**] or Raik [**157**]), by using the same test, showed that $M_{61}$ is prime in 1883. So Mersenne's list was known to Lucas in 1887 to be wrong; this should have discouraged Lucas' belief in it, but according to Tannery [**177**], Lucas looked at more of what Mersenne had written on this topic and attributed the following "proposition" to Fermat:

CONJECTURE 5.1. *For $2^p-1$ to be prime, it is necessary and sufficient that $p$ be a prime of one of the forms $2^{2n}+1$, $2^{2n} \pm 3$, $2^{2n+1}-1$.*

This is very close (without the attribution to Fermat) to the modern conclusion of Drake [**21**] concerning the numbers in Mersenne's list. Of course, under this rule, 61 should be included in the list. Possibly, then, Lucas rationalized that Mersenne's failure to include 61 was just an oversight. At any event the discovery of the primality of $M_{61}$ did not appear to shake Lucas' belief in Mersenne (Fermat), but it did seem to affect how he felt about $M_{127}$; for, he says in [**121**] that $M_{61}$ is the largest prime currently known, and in none of his subsequent publications does he ever mention that $M_{127}$ is a prime; he does however reaffirm in the year of his death (see [**122**, p. 376]) his belief that Mersenne was in possession of an important method. Today we believe, as did Tannery, that Mersenne's list is most likely an empirical result (see [**21**] or Heyworth [**47**]).

To confuse further this picture, we mention that in [**122**, p. 376] Lucas stated that he thought he had shown by very lengthy calculations that $M_{67}$ and $M_{89}$ are not primes. But according to Tannery [**178**], Lucas thought to the end of his life that $M_{67}$ was nevertheless a prime. As to why he included this statement about $M_{67}$ and $M_{89}$, we can again only speculate. Lucas had a correspondent named Reuss, and according to Fauquembergue [**25**], Reuss had written Lucas in January of 1877, saying that he had shown by using Lucas' test that $M_{89}$ is not a prime and that his (Reuss') computations required about 240 hours of work. In September of 1888, Reuss [**160**] wrote Lucas and informed him that he had shown that $M_{67}$ is not a prime. Fortunately, he lists his values of $S_1, S_2, \ldots, S_{66} \pmod{M_{67}}$ and we are able to see that he made an error in determining the value of $S_{22}$, and that all subsequent values are also incorrect. Thus, for the wrong reason, Reuss arrived at the correct conclusion. Possibly it was these computations that in some way confirmed Lucas' results and caused him to include the remark about $M_{67}$ and $M_{89}$ in his book.

The only explanation we can offer for Lucas' behaviour is that he did not believe the results of his own computations. Since he did not have faith in these calculations, he was unable to state anything consistent about the primality of $M_{127}$ or $M_{67}$. He praises Hudelot's work on proving $M_{61}$ a prime very highly, saying it is one of the most beautiful numerical memoirs that he has ever seen. Unfortunately, he seems to have little praise for his own calculations. This is a pity because he had almost certainly proved $M_{127}$ a prime and may very well have proved that $M_{67}$ is composite.

As a postscript to this section, we note that in 1894 Fauquembergue [**24**], by a then unpublished process of computation, declared that $M_{67}$ is composite. Later in 1912 he says in [**25**] that he used his device (see §4) to prove that $M_{67}$ is composite and it required only 20 hours of work to do this. Unfortunately, he did not publish his calculations as he did later for other numbers. Furthermore, in 1914 [**42**], he used his device to confirm that $M_{127}$ is a prime. In 1911, Powers [**148**] proved that $M_{89}$ is a prime (a result confirmed in 35 hours by Fauquembergue [**25**]) and in 1914 Fauquembergue also determined that $M_{107}$ is a prime. In fact, according to [**26**], he had proved $M_{107}$ a prime in February of

1914. Gérardin [**41**] states that Fauquembergue let him know of his result on June 7 of that year and that Powers [**149**] had communicated the same result (as determined by him) to the London Mathematical Society on June 11. However, in [**42**] Gérardin points out that Powers had cabled his result to Bromwich on June 1. Several of these computations were published in [**42**]. It is somewhat ironic that Fauquembergue should be the one to confirm Lucas' result on $M_{127}$. We do not have his calculations for $M_{67}$ and $M_{89}$, but of the six numbers that he investigated ($M_{101}$, $M_{103}$, $M_{107}$, $M_{109}$, $M_{127}$, $M_{137}$ in [**42**] and [**27**]) for which we do have his calculations, he gets the wrong answer for $S_{n-1}$ for four of them: $M_{101}$, $M_{103}$, $M_{109}$, $M_{137}$. (See Robinson [**162**]).

## 6. Lucas and necessity

In 1877, Lucas [**109**] turned his attention from tests for the primality of Mersenne numbers to those for the primality of the Fermat numbers $F_n$. In 1640 Fermat had conjectured that any number of the form $F_n = 2^{2^n}+1$ is prime. This is certainly the case for $n = 0, 1, 2, 3, 4$, but when $n = 5$, Euler showed in 1747 that 641 is a divisor of $F_n$. This is where matters stood when Lucas began to consider the question of the primality of $F_n$. In [**109**] he presented the following test (with some modifications and two misprints corrected):

THEOREM 6.1. *Let $F_n = 2^r+1$ ($r = 2^n$) and $T_1 = 3$. If we define the sequence $\{T_i\}$ by $T_{i+1} = 2T_i^2 - 1$ ($i = 1, 2, 3, \dots$), then $F_n$ is a prime if the first term of this sequence which is divisible by $F_n$ is $T_{r-1}$. Also, $F_n$ is composite if none of these terms up to $T_{r-1}$ is divisible by $F_n$. Finally, if $k$ denotes the rank of the first term which is divisible by $F_n$, the prime divisors of $F_n$ must have the form $2^{k+1}q+1$.*

Later in [**114**], Lucas gives this result in a somewhat different form (again with our modifications and corrections):

THEOREM 6.2. *Let $F_n = 2^r+1$ ($r = 2^n$) and $S_1 = 6 = V_2(2, -1)$. If we define the sequence $\{S_i\}$ by $S_{i+1} = S_i^2 - 2$, then $F_n$ is a prime when $F_n|S_k$ for some $k$ such that $r/2 \le k \le r-1$. Also, $F_n$ is composite if $F_n \nmid S_k$ for any $k \le r-1$. Finally, if $F_n|S_k$ with $k < r/2$, then any prime divisor of $F_n$ must have the form $2^{k+1}q+1$.*

One simple difference here from the earlier version is that $S_i = 2T_i$. But the more important difference is that primality is determined as soon as $F_n|S_k$ for $k \ge r/2$. We see, of course, that this easily follows from the statement of the previous version. For, if $k \ge r/2$, then

$$2^{k+1}q + 1 > 2^{2^{n-1}} + 1 > \sqrt{F_n},$$

which means that $F_n$ must be prime.

A few weeks after the appearance of [**109**], Pepin [**138**] noted that Lucas' test was only sufficient for the primality of $F_n$, but not necessary. He then proved that $F_n$ is a prime if and only if $5^{(F_n-1)/2} \equiv -1 \pmod{F_n}$. Pepin also noted that this could be made into a simple Lucas-like test by defining $T_1 = 5^2$, and $T_{i+1} = T_i^2$ ($i = 1, 2, \dots$). In this case, $F_n$ is a prime if and only if $F_n|T_{r-1}+1$. Pepin also mentioned that the number 10 could also be used here instead of 5. In this case the values of the $T_i$'s could be very easily evaluated as powers of 10. (In this remark Pepin demonstrates his ignorance of the actual use of these tests; for in usage, as noted by Lucas [**109**], we want to keep the values of our intermediate terms as small as possible. Hence, we compute them modulo the number being tested. Given this, no real advantage accrues on the use of 10 as opposed to 5.)

We should point out here that the test, often called "Pepin's test", today has a 3 in place of the 5 used above. Indeed, shortly after the appearance of Pepin's paper, Lucas ([**110**], [**114**, p. 313]) showed that any integer $a$ can be used for the 5 in Pepin's test as long as the Jacobi symbol $\left(\frac{a}{F_n}\right) = -1$. Actually, though, it was Proth [**153**] in 1878 who mentioned the use of the 3. He seemed, however, to be unable to give a complete proof of his result (in spite of the existence of [**110**]), but Lucas [**116**] later supplied him with one. Thus, the test that we call Pepin's test is actually Proth's test with a proof supplied by Lucas.

It appears that the first time Lucas ever came to grips with the problem of the necessity of his tests was when he read Pepin's paper. With respect to Lucas and necessity, Lehmer [**82**] stated the following:

> A great deal of confusion exists in Lucas's writings about the exact enunciation and actual proofs of these tests for primality. Nevertheless, it is evident that Lucas was in possession of the facts needed to prove the sufficiency of his tests. The confusion arose from the fact that he was unable or unwilling to consider the necessity also.

As we shall see, Lucas was certainly able to consider the problem of necessity, but he was rather strangely unwilling to do so in his tests. On this subject we allow Lucas to speak (with some minor errors corrected) for himself [**110**, p. 165]:

> Meanwhile one should observe that if the method indicated by Father Pepin leads to a form more clear and precise to state, which thus becomes similar to that of the Theorem of Wilson, it is preferable to keep for application to the form which we have adopted. For, the application of these theorems rests on a hypothesis, that of considering as prime a number of certain form taken arbitrarily; it is more likely to suppose, on the contrary, that the number is composite, as seems to be indicated by the assertion of Father Mersenne. As a consequence, instead of postponing the verification to the extreme limit by the use of quadratic nonresidues, it would be more practical to use one of the $\varphi(2^{2^{n-1}})$ numbers which belong to the exponent $2^{2^{n-1}}$ for

> the modulus $F_n$ considered as a prime. This cuts the process short by one half; but a direct search [for these numbers] is most difficult. Meanwhile one can assure oneself that by our previous procedure it suffices to demonstrate that $(F_2, F_3, F_4)$ are primes by executing respectively 3, 6, 12 operations instead of the maximum number of 4, 8, 16 which would be required by the other method; as to the numbers $F_5$ and $F_6$, they are composite.

Lucas seems to be a little confused here. He claims, rightly, that numbers of the forms under consideration are more likely to be composite rather than prime; but his test, like that of Pepin, must go to the extreme limit to verify this. This could be improved if one could solve a very difficult problem, but he doesn't know how to do it. Anyway, he concludes that his test works better on $F_2, F_3, F_4$ than does Pepin's. Although this all seems somewhat self-serving, it is curious to note that by using a modern result we can offer some support to his point of view. For, since

$$F_n = (2^{2^{n-1}})^2 + 1 = (2^{2^{n-1}} - 1)^2 + 2(2^{2^{n-2}})^2,$$

we can use a result of E. Lehmer [**97**] to show that if $F_n$ is a prime, then $F_n | S_t$, where $t \le r - 5$ $(n \ge 4)$. Thus, if $F_n$ is composite, Lucas' test could be modified to be possibly a little shorter than Pepin's. (But see the implementation of Pepin's test by Morehead and Western [**132**].)

We should add here that Lucas [**110**] used his test to show that $F_6$ is composite. Note that $F_6 = 2^{64} + 1$, one of the numbers Landry thought to be a prime. On learning of the composite nature of $F_6$, Landry set out to work on its factorization. After a labour of several months, and at the age of 82, he discovered by a rather clever method (see Williams [**187**]) adapted from his technique [**61**] for showing that $M_{31}$ is a prime, that $F_6$ is divisible by 274177 and that the other factor is a prime (see [**124**]). In 1905, Morehead and Western [**131**] independently used Proth's test $(a = 3)$ to show that $F_7$ is composite and in 1909, Morehead and Western [**132**], working together in one of the great feats of hand calculation (and perhaps the first example of a distributed computation in number theory!), showed that $F_8$ is composite by using a modification of this same test. Robinson [**162**] has verified by computer the correctness of this incredible piece of numerical work.

In spite of Lucas' lack of interest in the idea of necessity in practical applications, he did provide some tests that were both necessary and sufficient for the primality of Mersenne numbers. We mention two of these taken from [**115**].

THEOREM 6.3. *For $p = M_{4q+3}$ to be a prime, it is necessary and sufficient that*

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}} \equiv 0 \pmod{p}.$$

THEOREM 6.4. *For $p = M_{4nq+2n+1}$ to be a prime, it is necessary and sufficient that*

$$\left(2^n + \sqrt{2^{2n}+1}\right)^{\frac{p+1}{2}} + \left(2^n - \sqrt{2^{2n}+1}\right)^{\frac{p+1}{2}} \equiv 0 \pmod{p}.$$

We can only assume that Lucas left his tests in these forms because he was not really very interested in using them in any application. For, if one examines the first of these, one sees that

$$S_{4q+2} = V_{(p+1)/2}(1, -1) = \left(\frac{1+\sqrt{5}}{2}\right)^{\frac{p+1}{2}} + \left(\frac{1-\sqrt{5}}{2}\right)^{\frac{p+1}{2}};$$

that is, the test given in §3 is both sufficient and necessary for primality, contrary to a remark of Lehmer [**76**, p. 444]. It is difficult to believe that this simple fact escaped the notice of Lucas, but he never mentioned it.

The second of these tests is even more interesting; for, if we put $q = 0$, $\alpha = 2^n + \sqrt{2^{2n}+1}$, $\beta = 2^n - \sqrt{2^{2n}+1}$, we see that the theorem states that $p = M_{2n+1}$ is a prime if and only if

$$M_{2n+1} | V_{(p+1)/2}(2^{n+1}, -1).$$

If we put $S_i = V_{2^i}(2^{n+1}, -1)$ (a trick Lucas often uses), then

$$S_1 = V_2(2^{n+1}, -1) = 2^{2n+2} + 2 \equiv 4 \pmod{M_{2n+1}}.$$

Thus, if we put $S_1 = 4$ and define $S_k \equiv S_{k-1}^2 - 2 \pmod{M_{2n+1}}$ $(k = 2, 3, \ldots)$, we see that $M_{2n+1}$ is a prime if and only if $M_{2n+1} | S_{2n}$. This is the celebrated Lucas-Lehmer test for the primality of Mersenne numbers. Lucas seems to have known this test only as a sufficiency test (see [**124**]); it was Lehmer [**76**] who in 1930 showed that it was also necessary. Lucas had already done that in 1878, but his feelings about necessity blinded him to the result. This test has achieved a well-deserved fame. It is simple, elegant, and the means by which all of the large Mersenne primes have been verified. Many different proofs have been given for it (see [**186**] for references), the most recent being that of Rosen [**163**].

## 7. General primality tests

In [**106**] and [**114**, p. 302], Lucas presented the following theorem for primality testing.

THEOREM 7.1. *If $|\epsilon| = 1$, $p | U_{p+\epsilon}$, and $p \nmid U_k$ for all divisors $k$ of $p + \epsilon$ such that $k < p + \epsilon$, then $p$ is a prime.*

Lucas did not seem to be greatly interested in general primality tests, and did not, therefore, attempt to take this result much further. He did present in [**107, 110, 115**] and [**114**, pp. 309–311] a number of tests for numbers of the particular forms $N = Ar^n \pm 1$ $(r = 2, 3, 5)$, but these, of course, were such that $N + \epsilon$ could be easily factored. In spite of this favourable circumstance, several of his tests are not properly stated (in several of them he should have said something about limiting the size of $A$ to $A < \sqrt{N}$, but did not), and they often contain other minor errors.

Lucas has been criticized for his many errors and omissions, especially by Carmichael [**17**]; however, there can be no doubt that Lucas understood very well the basic principles behind his results. It is true that his statements and proofs thereof often leave something to be desired; but, on the other hand, these deficits are usually very easily repaired and do not require the machinery that Carmichael thought necessary. Indeed, it is the authors' opinion that Carmichael muddied the waters rather than clarified them; certainly his presentation lacks the charm and infectious enthusiasm that so characterizes Lucas' work. It should be kept in mind that during the brief time during which Lucas was developing his seminal work on primality testing (according to his publication list [**118**] and that of Harkin [**45**], this is represented by 13 papers published between January of 1876 and January of 1878) he wrote at least 70 papers on many other subjects. Considering this immense outpouring of activity during such a brief time period, it is easy to forgive him for the few easily correctable deficiencies that we have mentioned.

The Theorem of Fermat states that if $a$ is an integer and $p$ is a prime such that $p\nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$. Lucas knew that the strict converse of this theorem is false; for in [**110**] he gives the example $2^{37\cdot 73-1} \equiv 1 \pmod{37\cdot 73}$. In fact, in [**110**] he singles out the following particular case of the theorem given at the beginning of this section as the proper converse of Fermat's theorem.

THEOREM 7.2. *If $a^k - 1$ is divisible by $N$ for $k = N - 1$, and is not divisible by $N$ for any $k$ [$< N - 1$ and] a divisor of $N - 1$, then $N$ is a prime.*

It is strange that later in [**114**, p. 302] he presented this result in a weaker form.

THEOREM 7.3. *If $a^k - 1$ is divisible by $N$ when $k = N - 1$ and is not divisible by $N$ for $k < N - 1$, then $N$ is a prime.*

However, by the time he published his book, he had returned to the earlier result as the converse of Fermat's theorem (see [**122**, p. 441]). There is no evidence that Lucas ever used this result (even when $N - 1$ is easy to factor) to prove any numbers prime. This was possibly because he was unaware of a fast method for exponentiation (mod $N$) when the exponent is large, but this is difficult to believe because the technique is mentioned in Legendre's *Théorie des Nombres*, a book that Lucas must have read. Nevertheless, there is no indication in any of his published work that he knew of this device.

The next important contribution that was made to the problem of primality testing for a general $N$ was a remarkable half page of theorems (without proof) given by Proth [**152**] in December of 1878. We state the two most interesting of these below.

THEOREM 7.4. *$N$ is a prime if $N|a^n - 1$ for $n = N - 1$ and $\gcd(a^n - 1, N) = 1$ for every value of $n$ such that $n|N - 1$ and $n < \sqrt{N}$.*

THEOREM 7.5. *Let $N = m2^k + 1$, where $2\nmid m$ and $2^k > m$. If the Jacobi symbol $\left(\frac{a}{N}\right) = -1$, then $N$ is a prime if and only if $a^{(N-1)/2} \equiv -1 \pmod{N}$.*

Notice that the first of these is an improvement on Lucas' converse of Fermat's theorem, and the second is a generalization of the result of Pepin mentioned in §6. While no proofs of these results were offered, it is almost certain that Proth must have had correct proofs. He says in a letter to a Dr. Pein (see [**155**, p. 156]) that his proofs were long and that he did not have the time to copy them. The statements are correct as given, and it is difficult to believe that Proth would have had these correct statements if he did not have proofs, especially in the case of the first result which, as noted by Poulet in [**147**], even Dickson [**20**, p. 92] states incorrectly.

It is unfortunate that this work was never expanded upon; Proth certainly had intentions of doing this, but this remarkable, self-educated farmer was dead in January of 1879 at the age of 27 [**38**]. Also, because Proth was often guilty of making unsubstantiated claims (see, for example, [**151**]), it is likely that these results were ignored by many that might otherwise have taken up this work. As an interesting example of one of Proth's claims see [**154**] where it appears that he was aware of Gilbreath's conjecture [**50**] eighty years before Gilbreath. It seems that he thought he had a proof of it, something that still eludes us today.

The next important observation on this subject came from Pocklington [**144**] in 1914. He proves a result which can be stated as follows:

THEOREM 7.6. *If $N - 1 = q^n R$, where $q$ is a prime, $q\nmid R$ and for some $a$ we have $a^{N-1} \equiv 1 \pmod{N}$ and $\gcd(a^{(N-1)/q} - 1, N) = 1$, then each prime factor $p$ of $N$ is of the form $p = 1 + kq^n$.*

Notice that, although Pocklington was apparently ignorant of the work of both Lucas and Proth, he produced a result which is a generalization of their work. He was also aware that if one needed to evaluate $a^b \pmod{m}$ $(0 < a, b < m)$, then this could be done in $O((\log m)^3)$ elementary arithmetic operations; consequently, his test was computationally practical.

The computational model used by most number theorists today is that of "naive bit complexity". In this model, one can add two numbers of $n$ bits using $O(n)$ operations, multiply two $n$-bit numbers in $O(n^2)$ operations, etc. Pocklington seems to have been the first to analyze a number-theoretic algorithm using this model. In his 1910 paper [**143**], he gave an algorithm to find $\operatorname{ord}_p a$, the least positive $e$ such that $a^e \equiv 1 \pmod{p}$, when the prime factorization of $p - 1$ is known. He remarked:

> We notice that the labour required here is proportional to a power of the logarithm of the modulus, not to the modulus itself or its square root as in the indirect processes, and hence see that

> in the case of a large modulus the direct process will be much quicker than the indirect.

Perhaps Pocklington also deserves credit as the inventor of the randomized algorithm. In a 1917 paper [**145**], he gave an algorithm for computing square roots modulo a prime $p$ which used $O((\log p)^3)$ steps and observed "the labour varies roughly as the cube of the number of digits in the modulus, and so remains moderate for large moduli." His algorithm depended on finding a quadratic nonresidue of a special form by trial and error. He must have viewed this use of randomness as unsatisfactory, for he explained in a footnote:

> We have to do this [find the nonresidue] by trial, using the Law of Quadratic Reciprocity, which is a defect in the method. But as for each value of $u$ half the values of $t$ are suitable, there should be no difficulty in finding one.

In modern language, we would say that his method is a random polynomial-time algorithm, with each iteration having failure probability 1/2.

Pocklington's primality test was ignored for several years until D. H. Lehmer [**72**] realized its significance. Lehmer [**73**] also extended Pocklington's result to give the forms of the factors of $N/\delta$ in the case when $\delta = \gcd(a^{(N-1)/q}-1, N) > 1$, but his most important contribution was that of showing how these tests could be used in the actual practice of primality testing. In the course of doing this, he was able to demonstrate that large numbers which are not of simple forms like $Ar^n \pm 1$ could still be tested for primality fairly expeditiously. As an example we mention that in [**72**] Lehmer proved that $(10^{31}+1)/11$ is a prime. Lehmer's ideas will be discussed more fully in later sections, but in order to do this, we must now begin our discussion of the factoring problem.

## 8. Factoring

As has been mentioned earlier, the verification of a partial factorization of an integer $N$ into $N = ab$ with $a, b > 1$ is a much simpler process than the verification that a prime value of $N$ is indeed that. Nevertheless, the problem of factorization seems, at least empirically, to be much more difficult than that of primality testing. Also, of course, if a factorization algorithm is guaranteed, within a fixed bound on the time required, to find a nontrivial factor of $N$ and one is not found, then we have a primality test for $N$. Thus, progress on the factorization problem has always seemed to be somewhat less dramatic than on the primality testing problem. For example, we have already seen that Lucas was able to verify the primality of a 39-digit number in 1876, but it was only in 1970 (and by use of a computer) that it was finally possible to factor a 39-digit number (see Morrison and Brillhart [**133**]). It should be emphasized here that when we speak, as above, of factorization of a number $N$, the assumption being made is that the value of $N$ under consideration is not trivially factorable, i.e., $N$ has at least two large prime factors.

The first interesting factorization idea is that of Fermat [**28**] in 1643. (See also Henry [**46**].) We note that if $N$ is composite and odd, then $N = rs$ with $r, s$ odd and $r < \sqrt{N}$. If we put $a = (r+s)/2$, $b = (s-r)/2$, then $\sqrt{N} < a < (N+1)/2$ and $N = a^2 - b^2$. Thus, in order to factor $N$, one need only search values of $x = a^2 - N$ as $a = \lfloor\sqrt{N}\rfloor + 1, \lfloor\sqrt{N}\rfloor + 2, \dots, (N-1)/2$ until one finds a perfect square. This process can be simplified by using differences; that is, if we define $x_i = (\lfloor\sqrt{N}\rfloor + i)^2 - N$; $y_i = 2\lfloor\sqrt{N}\rfloor + 1 + 2i$, then $x_{i+1} = x_i + y_i$, $y_{i+1} = y_i + 2$.

Fermat also points out that one can shorten the search somewhat by rejecting any of the values of $x$ whose last few digits could not be those of a perfect square; for example, if the value of $x$ is 46619, then because the last two digits are 19 and there is no $b$ such that $b^2 \equiv 19 \pmod{100}$, then $x$ cannot be a perfect square. Thus, Fermat was aware of an idea that we will later call modular exclusion. It is this technique that Landry and Le Lasseur (see [**64**]) rediscovered and used to effect their factorizations. We emphasize that the method as presented here is really only going to be of some value when $r$ and $s$ are relatively close in value. If $s$ is very much larger than $r$, then the technique is very ineffective.

In 1798, Legendre proposed finding square-free values of $a$ such that there exist integers $x, y, z$ for which

$$x^2 - kNz^2 = ay^2. \tag{8.1}$$

Notice that regardless of the value of $k$, if $p$ is any prime divisor of $N$, then the Legendre symbol $\left(\frac{a}{p}\right) = 1$. For a given $a$ such values of $p$ can only have certain linear forms; for example, if $a = 2$, then $p \equiv \pm 1 \pmod 8$; if $a = 3$, then $p \equiv \pm 1 \pmod{12}$; and if $a = 5$, then $p \equiv \pm 1 \pmod 5$, etc. Legendre tabulated these forms for various values of $a$.

If, for example, we could solve (8.1) for $a = 2, 3, 5$, then if $p|N$, we must have $p \equiv 1, 49, 71, 119 \pmod{120}$. As any prime ($\neq 2, 3, 5$) can be congruent modulo 120 to $\varphi(120) = 32$ possible values, we see that this knowledge allows us to reduce the amount of possible trial division by a factor of 8. In general, if we have $r$ such independent conditions, the number of trial divisions of $N$ can be reduced to about $2^{-r}\pi(\sqrt{N})$ trials, where by $\pi(x)$ we mean the number of primes which do not exceed $x$.

In 1929, D. N. Lehmer [**94**] and D. H. Lehmer (see [**89**]) produced a set of factor stencils which could be used to factor numbers up to $48593^2 = 2361279649$. For each value of $a$ up to 250 in absolute value, a stencil was created as a matrix of 100 rows and 50 columns. A hole was punched in any spot corresponding to those of the first 5000 primes for which $a$ is a quadratic residue; that is, $\left(\frac{a}{p}\right) = 1$ for these particular primes $p$. (D. N. Lehmer considered 1 to be a prime; thus, his first 5000 primes begin at 1 and end at 48593). The stencils were approximately 20cm by 43cm, and were provided in a wooden box with a glass cover. To use the stencils (see [**95**]), one first discovers the values of $a$ such that $|a| < 250$ and (8.1) is solvable. Then the corresponding stencils are stacked on top of each other and placed on top of the glass cover. An electric light is then introduced into the box to shine through the holes (an early example of a user interface!). These holes correspond to the only possible primes that could divide $N$. In 1939, Elder [**22**] put these stencils on 2000 Hollerith cards (i.e., IBM punch cards).

There may be a question about the use of $k$ in (8.1). Normally one would think that $k$ could simply be put equal to one, but it is often convenient to use other values of $k$, especially if $\left(\frac{N}{p}\right) = -1$ for many of the smaller primes, in order to solve (8.1). Today we call these values of $k$ 'multipliers'. They are used rather extensively in certain factoring techniques.

We are now left with the problem of how to solve (8.1). Legendre suggested using the continued fraction expansion of $\sqrt{kN}$. For if

$$\text{(8.2)} \qquad \sqrt{kN} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{\theta_n}}}}}$$

where $\theta_n = (P_n + \sqrt{kN})/Q_n$ $(P_n, Q_n \in \mathbb{Z})$, then $0 < Q_n < 2\sqrt{kN}$ $(n > 0)$, and we can use the values of $q_0, q_1, \dots, q_{n-1}$ to compute easily integers $A_{n-1}, B_{n-1}$ such that

$$\text{(8.3)} \qquad A_{n-1}^2 - kNB_{n-1}^2 = (-1)^n Q_n.$$

Thus, $a$ can be taken as the square-free part of $(-1)^n Q_n$. For the purpose of this technique, however, we shall see that there is no need for the coefficient of $kN$ in (8.1) to be a perfect square. We would be content to know that there exists a value of $x$ such that

$$\text{(8.4)} \qquad x^2 \equiv a \pmod{N}.$$

Such values of $a$ are called quadratic residues of $N$. The determination of small (in absolute value) quadratic residues of $N$ is still considered to be a very difficult task. We shall discuss this further in what follows.

We conclude this section by mentioning a very important observation of Gauss [**30**, Art. 320]. Suppose $f(x), g(x) \in \mathbb{Z}[x]$, and we wish to solve the Diophantine equation

$$\text{(8.5)} \qquad f(x) = g(y)$$

for integers $x$ and $y$. (Gauss only treats the equation $a + mx = y^2$, but the idea applies more generally.) Select different (exclusion) moduli $E_1, E_2, \dots, E_r$. We must have $f(x) \equiv g(y) \pmod{E_i}$ for $1 \le i \le r$ for any solution $(x, y)$ of (8.5). For each value, then, of $y = 0, 1, 2, \dots, E_i - 1$, find the possible residues classes for $x$ modulo $E_i$. Combine these to find the permissible residue classes for $x$ modulo the least common multiple of the $E_i$'s.

To use Gauss' example, suppose we want to solve $22 + 97x = y^2$. We consider $E_1 = 3$, $E_2 = 4$, $E_3 = 5$, $E_4 = 7$. Permissible values of $x$ modulo $E_1$ are $0, 2$; modulo $E_2$ are $2, 3$; modulo $E_3$ are $1, 2, 4$; and modulo $E_4$ are $0, 1, 4, 6$. It is easy to see that the least integer satisfying all of these is 11, and in fact $22 + 97 \cdot 11 = 33^2$. Notice that with one exception the $E_i$-values here are distinct primes; thus, on using a new $E_i$-value, we eliminate about half of the previous candidates for $n$ in this problem. In subsequent sections we shall illustrate the importance of Gauss' idea of exclusion. We should mention that Gauss had several other ideas for factorization techniques (see [**30**, Arts. 329–334]), but only the exclusion idea has turned out to be of real practical importance.

## 9. Seelhoff and Pepin

In this section we discuss some of the important work on factorization techniques done by two individuals whose contributions appear to have been largely ignored. We use the term 'appear' here because it is not entirely clear whether or not their work was taken over and expanded by others. In any event their ideas were important and merit some attention.

Between the years 1885 and 1887 Paul Seelhoff published a number of papers on factorization and primality testing. Some of this work was not of very high quality (we have already mentioned his less than adequate proof of the primality of $M_{61}$), but at least one of his papers contained some interesting ideas.

In [**166**] he presented a method of factorization which first requires that for a given $N$ we find a number of different values of $a$ such that (8.4) holds. He attacked this problem by putting $N = \omega^2 + r$, where $\omega = \lfloor \sqrt{N} \rfloor$. If $p$ is any prime such that $\left(\frac{N}{p}\right) = 1$, solve $\rho^2 \equiv N \pmod{p^k}$ and put $\alpha = \omega \pm (\rho + yp^k)$. We then have $N = (\omega - \alpha)^2 + b$, where $b = \alpha(2\omega - \alpha) + r$ and $p^k | b$. The point here is that, if the $|\alpha|$-values are near $p^k$, then the corresponding $b$-values will tend to be of size about $2p^k\sqrt{N}$, and since they are already divisible by $p^k$, they should be somewhat easy to factor. On putting $b = at^2$, we have a value of $a$ satisfying (8.4).

Seelhoff suggested that for values of $N$ of about 15 digits, the values of $p^k$ to try are the primes from 7 to 97 with $k \le 2$; 5 with $k \le 4$; 3 with $k \le 6$; and 2 with $k \le 10$. (Of course, only those primes $p$ for which $\left(\frac{N}{p}\right) = 1$ would be used.)

His next step is best illustrated by using an example. He selected for that purpose $N = 7 \cdot 2^{34} + 1$ and took as his collection of possible values of $p$ the set

$$\{2, 5, 7, 11, 19, 31, 37, 47, 53, 67, 71, 93, 127\}.$$

We have $N = 346783^2 + 635200$.

After several trials he found that for

$$\alpha = 1950 \quad (\alpha \equiv 0 \pmod{5}, \alpha \equiv 581 \pmod{37^2});$$

$$\alpha = 143432 \quad (\alpha \equiv 3 \pmod{11}, \alpha \equiv 14400 \pmod{127^2});$$

$$\alpha = -3836 \quad (\alpha \equiv 3 \pmod{11}, \alpha \equiv 271 \pmod{37^2})$$

one has

$$\begin{aligned} N &= 344833^2 + 2 \cdot 7 \cdot 11 \cdot 2960^2 \\ &= 203351^2 + 7 \cdot 106172^2 \\ &= 350619^2 - 2 \cdot 11 \cdot 11026^2. \end{aligned}$$

From the first two of these he obtained

$$11 \cdot 832082029^2 \equiv 2 \cdot 150479740^2 \pmod{N}.$$

He combined this with the third and found

$$5045995048467^2 \equiv 26380527979530^2 \pmod{N}$$

or

$$N|(5045995048467 - 26380527979530) \times (5045995048467 + 26380527979530).$$

In fact, $\gcd(5045995048467 - 26380527979530, N) = 317306291$ and $N = 379 \cdot 317306291$. Those who are familiar with modern factoring techniques will be struck by the similarity of this method to those which make use of the idea of combining congruences, such as the Quadratic Sieve and CFRAC (see below). Of course, we have more sophisticated methods now for effecting the divisions needed to determine the $a$-values (indeed, no divisions need be performed if the techniques of the Quadratic Sieve are employed) and for assembling the dependencies[5] in order to get values of $x$ and $y$ such that $x^2 \equiv y^2 \pmod{N}$, but Seelhoff seems to have understood the basic idea behind some of our modern methods back in 1886. He used his method [**167, 170**] to factor some numbers of the form $A2^n + 1$, as he was interested in these as possible factors of Fermat numbers.

Father Théophile Pepin S.J. is best known today for the primality test which bears his name. However, Pepin did a lot of work on factoring. His most useful techniques, one of which we will discuss here, was pretty well developed in 1890 (see [**139**]), but in a series of papers [**140, 141, 142**] (see Statuti [**174**] for a partial bibliography of Pepin's work) he continued to refine and apply it to various numbers of the form $(a^n - 1)/(a - 1)$. Numbers of this type were of particular interest to Pepin because of their importance in the study of perfect numbers.

To factor $N = (a^n - 1)/(a - 1)$ with $n$ odd, we first notice that $N$ is odd and that if $p|N$, then $p \equiv 1 \pmod{2n}$. We now consider the more general problem of factoring any odd $N$ whose factors must be of the form $2nx + 1$ with $n$ odd. We first demonstrate that $N$ has no prime factor less than or equal to $m$ (by trial division, say).

[5] By a *dependency* we mean a collection of possible values for $a$ whose product is a perfect integral square. In the previous example the product of $-2 \cdot 7 \cdot 11$, $-7$, $2 \cdot 11$ is the perfect square $(2 \cdot 7 \cdot 11)^2$.

Suppose $N = s_1 s_2$; since $s_2 > m$, we have $N/(ms_1) > 1$; hence $0 < s_1 - m < (s_1 - m)N/(ms_1)$ and $s_1 + s_2 = s_1 + N/s_1 < m + N/m$.

Furthermore, by using the results at the beginning of §8, we also see that $s_1 + s_2 > 2\sqrt{N}$. If we put $L = m + N/m$, $s_1 = 2nx + 1$, $s_2 = 2ny + 1$, we get

$$\frac{\sqrt{N} - 1}{n} < x + y < \frac{L - 2}{2n}. \tag{9.1}$$

Also, since $4n^2xy + 2n(x + y) = N - 1 = 2nN'$, it follows that if $N' = 2nN'' + r$, then

$$x + y = r + 2nz. \tag{9.2}$$

Putting $x - y = u$ and noting that $4xy = (x + y)^2 - (x - y)^2$, we get

$$(2nz + r)^2 - u^2 + 4z = 4N''.$$

If $2|r$, we can replace $u$ by $2u'$ and divide by 4. In any event, we get an expression of the form

$$az^2 + 2bz + c = u^2, \tag{9.3}$$

where $a, b, c$ are known integers and the value of $z$ is bounded by using (9.1) and (9.2). So far, all this really represents is a more sophisticated version of the difference of squares method of Fermat. The equation (9.3) is a Diophantine equation which can be solved by using Gauss' method of modular exclusion.

As one of several examples of his method, Pepin considered $N = (5^{13} - 1)/4 = 305175781$. Since any prime divisor of $N$ is of the form $26x + 1$ and since there is no such prime divisor less than 1000, he was able to say that if $N = (26x + 1)(26y + 1)$, then $1343 < x + y < 5946$. Furthermore, $26xy + x + y = (N - 1)/26 = 11737530$; hence, $x + y = 26z + 12$ and

$$169z^2 + 157z - 451407 = u^2 \tag{9.4}$$

with

$$51 < z < 229. \tag{9.5}$$

Using $8, 9, 5, 7, 11, 13$ as exclusion moduli, he found, by using a technique like the Sieve of Eratosthenes, that there are no candidates for $z$ satisfying (9.4) and (9.5). Thus, $N$ is a prime.

Pepin went on to factor many numbers by using this technique or some variant thereof. If one examines [**62**] in the light of [**64**] it seems that Landry must have used a technique very like this to effect his factorizations in [**63**]. Indeed, in 1880 Landry [**65**] essentially proved that if $p$ is any prime and $N \equiv a^2 - b^2 \pmod{p}$, then there are precisely $(p + (\frac{N}{p}))/2$ possible values of $a$ modulo $p$. This, of course, is why the exclusion principle works; each additional prime exclusion modulus cuts the number of possible values for $a$ to one half their former number. It is possible that Pepin's ideas did not receive the currency they merited because of the rather obscure journals in which they were published. The method, however, became the most important factorization technique until well after the arrival of computers.

## 10. An example of Cole

In §5 we mentioned that Fauquembergue (and possibly Lucas) had shown by 1891 that $M_{67}$ is composite. In 1903, Cole [**19**] succeeded in finding the factors of $M_{67}$. This marvelous feat of hand calculation has been justly celebrated through the story related by Bell [**9**].

> I should like here to preserve a small bit of history before all the American mathematicians of the first half of the twentieth century are gone. When I asked Cole in 1911 how long it had taken him to crack $M_{67}$, he said "three years of Sundays." But this, though interesting, is not the history. At the October, 1903, meeting in New York of the American Mathematical Society, Cole had a paper on the program with the modest title *On the factorization of large numbers*. When the chairman called on him for his paper, Cole — who was always a man of very few words — walked to the board and, saying nothing, proceeded to chalk up the arithmetic for raising 2 to the sixty-seventh power. Then he carefully subtracted 1. Without a word he moved over to a clear space on the board and multiplied out, by longhand, $193,707,721 \times 761,838,257,287$. The two calculations agreed. Mersenne's conjecture — if such it was — vanished into the limbo of mathematical mythology. For the first and only time on record, an audience of the American Mathematical Society vigorously applauded the author of a paper delivered before it. Cole took his seat without having uttered a word. Nobody asked him a question.

(Given Bell's accuracy on other matters, aspects of this story may be apocryphal.) What seems to be much less known is how Cole actually achieved this factorization. He appears to have been unaware of Fauquembergue's work, but he did take seriously Lucas' comment in [**122**] concerning the composite character of $M_{67}$. It was this that caused him to seek its factors. He began by finding a collection of quadratic residues of $M_{67}$. These he listed as

$$2, -3, -7, 13, -23\cdot 53, 37, 41, 61, -67, -71, 23\cdot 83, 89, 97, 101, \ldots$$

etc. He did not say exactly how he discovered these, but as he refers to the work of Seelhoff mentioned in §9, he likely used Seelhoff's technique. He made the important observation (refined later by Kraitchik) that if a prime $r$ (taken with the proper sign) is a quadratic residue of $N$, then there can be at most $(r+3)/4$ possible values of $a$ modulo $r$ satisfying $N \equiv a^2 - b^2 \pmod{r}$. Notice that this is an improvement on the upper bound of $(r+1)/2$ mentioned in §9.

Next, by using the same reasoning as Euler concerning $M_{31}$, he noted that any prime factor of $M_{67}$ must be of the form $536k+1$ or $536k+135$. Since $-3$ is a quadratic residue of $M_{67}$, these forms can be further refined to $1608k+1$ or $1608k+1207$. By using these forms and some of his other quadratic residues of $N$, he eliminated (but not entirely convincingly) all possible prime factors $< 16000000$.

He then attempted to solve $N = a^2 - b^2$. He found that

$$\begin{aligned}
a &\equiv 671 \pmod{67^2},\\
a &\equiv 0 \pmod{8},\\
a &\equiv 1, 4^* \pmod{5},\\
a &\equiv 1, 3^* \pmod{7},\\
a &\equiv 0, 1^*, 12 \pmod{13},\\
a &\equiv 10, 37, 46^*, 64 \pmod{81}.
\end{aligned}$$

There are 48 possible residue classes here for $a$ modulo $1323536760 = 8\cdot 5\cdot 7\cdot 13\cdot 81\cdot 67^2$, but only one is the correct one. After what must have been a great deal of work, Cole selected that class indicated by the asterisks; that is, $a = 1323536760x + 1160932384$. This was used to find an equation like (9.3). The exclusion moduli $23, 37, 41, 53, 61$ were then used to narrow $x$ down to 287 from which Cole obtained $a = 381015982504$, $b = 380822274783$ and his factorization.

## 11. The sieve

During the years 1894–1897, Lawrence [**66, 67, 68**] rediscovered the difference of squares technique and some of Pepin's refinements to it. In fact in [**68**], he was able to use his method to prove that the factors of $10^{29} - 1$ and $10^{25} - 1$ found by Looff [**100**] are primes. However, the most important contribution of Lawrence occurs in [**67**], where he discussed a means of mechanizing the process of solving (9.3) by the use of exclusion moduli. He first described a technique for doing this that made use of moveable paper strips, but it is his second idea which is really of interest to us here. He suggested the construction of a machine in which gears of $m$ teeth would be used for each exclusion modulus $m$; thus, each such gear would represent (as it rotates) an endless paper strip. The gears (each with the same tooth size) would be driven by the same driving gear, and, as they would be of differing diameters, would have to be mounted on different shafts. The teeth on each $m$-toothed gear would be numbered $0, 1, 2, \ldots, m-1$, and a brass stud would penetrate through it at the point(s) of an acceptable (mod $m$) residue (one for which (9.3) could hold for $z$ (mod $m$)). When studs from each of the gears were all in contact a circuit would be completed and a bell would ring or the machine would stop, indicating to the operator that a solution of (9.3), modulo the least common multiple of the exclusion moduli, had been detected. Of course, in order to determine the $z$-value, a count would have to be recorded of the number of rotations of the driving gear.

Several other details for the construction of this machine are also provided, but it seems that Lawrence never actually built such a device, being instead content simply to describe it in principle. His description is not complete, as he admitted, but it is sufficient to convince anyone that the basic idea of mechanizing the modular exclusion principle for solving (9.3) is a real possibility.

This idea of mechanizing the solution of (9.3) seems to have been forgotten until 1912, when a flurry of activity, apparently inspired by Andre Gérardin, began to produce some results. This may have originated through Gérardin's publishing in 1910 a French translation of Lawrence's paper [**67**] in his peculiar journal/newsletter called *Sphinx-Oedipe*. The first machine announced was that of Maurice Kraitchik in February of 1912 [**37**]. Kraitchik had read the version of Lawrence's paper which was published in *Sphinx-Oedipe* because he [**52**] refers to it in an earlier issue. Furthermore, the machine, when it is described in [**39**] (or in somewhat less detail in [**53**, pp. 43–44]), is rather similar to that of Lawrence, except that the gears representing the various exclusion moduli are each mounted on the same shaft. Also, he mentions the possibility of putting holes in the gears (instead of studs) and shining light through onto a screen. When a spot of light appears on the screen a solution has been detected. (Holes that did not represent a possible solution, of course, would have to be plugged.) Curiously, however, Kraitchik never refers to Lawrence's work in this connection.

In March of 1912, Gérardin [**37**] refers to machines of Pierre Carissan, Kraitchik, and himself. Kraitchik's machine is described in some detail in April of 1912, but the descriptions of Carissan's (built by his brother Eugène-Olivier) and Gérardin's machines, given respectively in [**16**] and [**40**], are rather vague. It appears that each of these machines existed only as a prototype and that none ever produced any important result. Later in 1913–14, E.-O. Carissan built another model of such a mechanism and was so encouraged by its performance that he decided to have a precision device constructed. Unfortunately, World War I intervened, and his device was not completed until 1919. This seems to have been the first automatic sieve mechanism to have ever been successfully constructed. A full and convincing description of it is given in [**16**]. It is also mentioned again by d'Ocagne [**135**] in his lengthy paper on calculating machines. Indeed it is rather a telling point that neither Kraitchik's nor Gérardin's machines are described by d'Ocagne.

Carissan's machine was made up of 14 concentric metallic rings representing the exclusion moduli: $19, 21, 23, 26, 29, 31, 34, 37, 41, 43, 47, 53, 55, 59$. A pinion gear whose axis was parallel to the plane of the rings drove all of them at the same rate. Each ring had a number of equidistant studs on the upper side. The number of such studs was equal to the appropriate exclusion modulus. Those studs representing a possible solution were covered by a nonconducting cap. When these passed under a 'line of investigation', a circuit would be completed when a solution (each stud under the line was capped) appeared and a sound would be made in a telephonic receiver placed on the ear of the operator, alerting him to the solution.

While this device was hand-driven, plans were also made to construct a machine-driven model; however, this seems never to have been done. The hand-driven device ran through the numbers at the rate of 35-40 per second. A counter (up to 1000000) would keep track of how many numbers had been sieved. As an example, we mention that the machine required only 15 minutes to prove that $M_{31}$ is a prime.

Unfortunately, Pierre Carissan died in 1923, and E.-O. Carissan died in 1925, events that likely contributed greatly to their pioneering sieve not receiving the attention that it deserved. The machine itself languished in a drawer in the Observatoire de Floirac (near Bordeaux) for many years. It was inspected there by the authors several times. Recently, France Silber, a daughter of E.-O. Carissan, took possession of the machine, and there is hope that it will soon be donated to the collection of the Conservatoire National des Arts et Métiers. We are extremely grateful to Marie-Josèphe Salefran-Carissan and France Silber for informing us of the sieve's location.

The next individual to look at the problem of constructing number sieves was D. H. Lehmer [**74**]. Lehmer was unaware of the work of the Carissans and remained so until 1989. In fact in his paper [**81**, p. 663] on sieves he states the following:

> The literature contains at least two descriptions of such machines which, though impractical in their design, are theorcticaily interesting. As far as the writer knows, the first successful machine of this type was constructed by him in 1927.

Lehmer was referring to the machines of Lawrence and Kraitchik here. In fact it is rather strange that he gives so very little credit to them, especially since his photoelectric sieve of 1932 represents in many ways the fruition of their ideas; however, Lehmer had determined that neither of these earlier mechanisms, as described, would actually work and therefore decided to maintain a discrete silence concerning them and their creators. His device, described in [**79, 81**], would search through numbers at the rate of 5000 per second. In constructing this remarkable machine, Lehmer pushed contemporary technology about as far as he could. For a charming description of the function of it we refer the reader to the paper [**96**] of Lehmer's father, D. N. Lehmer.

As it would take considerable space to discuss all of Lehmer's work on sieves, we simply provide below a list of all sieves known to the authors at present. All, but those of Carissan and Gérardin (see [**43**]) and the last four are Lehmer's. For a more detailed account on sieves and their history we refer the reader to the paper of Stephens and Williams [**175**] and Patterson [**137**].

### Sieve Systems

| Machine | Year | Rings | Trials/Sec |
|---|---|---|---|
| E. Carissan | 1919 | 14 | 35-40 |
| Bicycle Chain | 1926 | 19 | 50 |
| Optical Gears | 1932 | 30 | 5,000 |
| 16 mm Movie Film | 1936 | 18 | 50 |
| A. Gérardin | 1937 | ? | < 10 |
| SWAC† | 1950's | ? | 1,450 |
| IBM 7094† | 1960's | 21 or 22 | 100,000 |
| DLS-127 | 1966 | 31 | 1,000,000 |
| DLS-157 | 1969(?) | 37 | 1,000,000 |
| ILLIAC IV† | 1960's | 64 | 15,000,000 |
| Shift Register | 1975 | 42 | 20,000,000 |
| UMSU | 1983 | 32 | 133,000,000 |
| OASiS | 1989 | 16 variable | 215,000,000 |
| Sun4/280† | 1989 | 32 | 2,000,000 |
| SSU | 1991 | 30 | 200,000,000 |

† Denotes software running on a general purpose computer.

It may interest the reader to learn that up to 1970 these sieve methods were still the fastest techniques known for factoring. In fact the DLS-127 was used to factor a 33-digit divisor of $2^{136}+1$ in 2600 hours (see [**13**, p. lvi]). In spite of the successes of these cheap, easy-to-construct, and useful mechanisms, their history has been characterized by a lack of interest or neglect. Indeed, in speaking about the sieve problem in his paper [**88**, p. 456] on the history of the sieve process, Lehmer stated:

> It's very esoteric, of course, and since I am practically the only man working in this field you can see how widespread the interest in it is.

The situation is not much different today, and that is a great pity; there's a lot you can do with a sieve. Possibly the current easy availability of off-the-shelf computer chips and components will cause modern researchers to begin to investigate the problem of construction and utilization of number sieves. We certainly hope so.

## 12. Kraitchik and Lehmer

In 1911, only one number from Landry's original table of factorizations of $2^n \pm 1$ $(n \leq 64)$ remained to be factored; this was $N = (2^{61}+1)/3$. Gérardin [**36**] posed the factorization of this number as a contest in May of that year. A then new contributor to *Sphinx-Oedipe*, Kraitchik, first suggested the following conjecture:

CONJECTURE 12.1. *If $2^n - 1$ is prime, then $(2^n+1)/3$ is also prime.*

Later [**51**] he found that there were no factors of $N$ between $\lfloor\sqrt{N}\rfloor = 876706528$ and 61003051. Finally, Poulet [**146**] proved that $N$ could have no prime factor less than 68200400, and thus $N$ is a prime. Poulet also pointed out that Kraitchik's conjecture is false, as it fails for $n = 89$. Much more recently a revised form of this conjecture has been suggested by Bateman, Selfridge, and Wagstaff [**6**]. Their conjecture reads as follows:

CONJECTURE 12.2. *If two of the following statements about an odd positive integer p are true, then so is the third one:*

- $p = 2^k \pm 1$ *or* $p = 2^{2k} \pm 3$.
- $M_p = 2^p - 1$ *is a prime.*
- $(2^p+1)/3$ *is a prime.*

This has been verified for all primes $p$ up to 100000. Incidentally, it was in [**6**] that the number $(2^{2539}+1)/3$, mentioned in §1, was identified as a probable prime.

This debut of Kraitchik into the factoring business was followed over ten years later by the publication of several books containing a great deal of information about number theory in general and factoring in particular. In [**53**, Chapter 6], he described in detail how he factored the 19-digit number $2^{61} + 2^{31} + 1$. He used a method which is little more than a minor refinement of the technique of Pepin and Lawrence, but does not attribute the technique to either of them. This is peculiar because, as we have already seen, he was aware of Lawrence's work, and he must have known about Pepin's work through a description of it by Gérardin [**35**] published in *Sphinx-Oedipe*. Furthermore, Cole's paper [**19**] had also appeared in French translation in 1910 in *Sphinx-Oedipe*.

Kraitchik also stated in [**53**] that he proved that $(10^{19}-1)/9$ is a prime, but this had already been done earlier by Hoppe [**48**] in 1918. Kraitchik became quite adept at using a modified version of Lawrence's technique of moveable strips in order to effect his factorizations. As a result of this skill, he was able to factor several large numbers such as: $2^{68}+1, 2^{53}+2^{27}+1, 2^{122}+1, 2^{77}-1$.

In 1851, Looff [**100**] published a table of factors of numbers of the form $10^n - 1$. These same factorizations for $n \leq 42$ and with some addenda were reported later by Reuschle. There were several holes in Reuschle's tables, namely for $n = 17, 19, 23, 25, 27, 29, 31, 33, 34$ (because of 17), $35, 37, 38, 39, 40, 41$, where the factorizations were incomplete. Le Lasseur (see Lucas [**117**], Brocard [**14**]) factored $(10^{17}-1)/9$ in or before 1879; we have already seen that Lawrence and Hoppe had found $(10^{19}-1)/9$ to be prime in 1918. This was how matters stood until 1926 when Lehmer [**72**] turned his attention to the factorization of the 15-digit value of $N = (10^{27}-1)/(3^5 \cdot 37 \cdot 757 \cdot 333667)$. He was able to use his primality testing ideas to prove $N$ a prime. He did this by first factoring

$N - 1 = 2 \cdot 5 \cdot 3^3 \cdot 31249 \cdot 52189481$ and then showing that $3^{N-1} \equiv 1 \pmod{N}$ and $\gcd(3^m - 1, N) = 1$, where $m = (N-1)/52189481$. Hence any prime divisor of $N$ must be of the form $52189481k + 1$. Since $\sqrt{N} < 20984153$, $N$ must be a prime. He also showed that $(10^{19} + 1)/11$ is a prime and computed the value of $3^{N-1}$ for $N = (10^{20} + 1)/(10^4 + 1)$ and $N = (10^{23} - 1)/9$. In both cases he obtained values of $3^{N-1} \pmod{N}$ different from 1 and concluded that both of these numbers must be composite. Later, using his bicycle chain sieve, he [**74**] was able to factor $(10^{20} + 1)/(10^4 + 1)$.

Lehmer's most impressive computation [**78**], however, was rather modestly announced in June of 1932. Kraitchik [**55**, p. 142] stated in 1926 that he had shown in 1922 (by use of the Lucas-Lehmer test) that the last number in Mersenne's list, $M_{257}$, is composite. However, he provided no details of this Herculean labour except to say that it required the months from August to December of 1922 to complete the work. Kraitchik's book appeared after July of 1926; in June of that same year Lehmer (unaware of Kraitchik's work) began the task of investigating the 78-digit $M_{257}$. He made use of a 10-digit calculating machine and his cross division process [**70**], a modification of an idea of his father [**91, 93**], to effect the computations. He also checked each value of $S_i$ by repeating the calculations modulo 1001. Here we use $S_1 = 4$, $S_i \equiv S_{i-1}^2 - 2 \pmod{M_{257}}$, for $0 \le i < 257$.

On March 6, 1927 he found that $S_{256} \neq 0$. Lehmer did not publish this finding, although he did publish in [**71**] his discovery that $M_{139}$ is composite; indeed, he began his work on $M_{257}$ less than a month after he completed his work on $M_{139}$ and he used the same techniques. Possibly, he was forestalled by the appearance of [**55**] or he was unsure of the accuracy of his calculations. We know nothing more about this until we read in Kraitchik [**56**, p. 83] that Lehmer found that he had made an error in the 47th term (in fact, it was $S_{48}$ that was wrong) of his calculations. According to the dates Lehmer provides in his journal, this meant that all the work from August of 1926 to March of 1927 had been in vain. Lehmer had also asked Kraitchik for a copy of his computations; however, Kraitchik said that he had sent them to Gérardin without keeping a copy for himself. On being requested to return them, Gérardin declared that owing to the state of his health, he could not at that time recover Kraitchik's calculations from among the thousands of kilograms of archives in his possession. These calculations have still not been located to this day. Later, when Lehmer visited Gérardin, he discovered why a search of Gérardin's papers might prove hazardous to anyone's health. The entire office was full of papers piled up everywhere and in no apparent filing system.

Actually, it was Lehmer's wife Emma who had detected the error in $S_{48}$. At Lehmer's request she began in 1930, starting at $S_{47}$, to redo the calculations. The values of $S_i$ were now checked modulo $10^8+1$ and modulo $10^9+1$. Unfortunately, this work in Lehmer's journal is not dated as frequently as the earlier work; we only know that $S_{128}$ had been computed on September 17, 1930. Both Lehmer and his wife shared the computational chores until $S_{256}$ was computed. This time, as noted later by Robinson [**162**], the calculation of $S_{256}$ was correct. Lehmer was able to announce in June of 1932 that $M_{257}$ is composite. According to Reid [**158**] this computational feat required over 700 hours of work, whereas the determination of the composite character of $M_{149}$, also announced in [**78**], had required only 70 hours.

Kraitchik and Lehmer went on to improve their techniques and produce other factorizations. A glance at the tables of factors of $2^n \pm 1$ in Kraitchik [**56**, pp. 84–88] (but see Lehmer [**84**, pp. 29–30]), [**58**, pp. 12–13; 38–39], [**59**] and [**85**] will give the reader some idea of the strength of both their methods and their endurance. By using his sieves, Lehmer was able to achieve his factorizations more rapidly than Kraitchik; for example, see [**80**], where Lehmer used his photoelectric sieve to factor 5 difficult numbers, one of 21 digits, in a matter of a few hours. Naturally, both of these authors made errors in their calculations from time to time; this is only to be expected, but Kraitchik made a serious mathematical error which, taken with some simple calculation mistakes, led him to the belief that certain numbers such as $(2^8+1)(2^{120}+1)/((2^{24}+1)(2^{40}+1))$ were prime when they are not.

## 13. Quadratic Residues and a "Fallacious Principle"

In many of his attempts to factor (or primality test) an integer $N$, Kraitchik was first very concerned about determining a collection of quadratic residues of $N$. His techniques for finding these quadratic residues are fully described in [**55**, pp. 123–132] and again in [**58**, pp. 134–138]:

For a given $N$ find small integers (say primes $\le 50$) $r_1, r_2, r_3, \ldots$ for which $\left(\frac{N}{r_i}\right) = 1$. Then find values of $x$ such that the difference $R = \pm(x^2 - N)$ is divisible by $r_1, r_1^2, r_1^3, \ldots, r_2, r_2^2, r_2^3, \ldots, \ldots r_1^2 r_2^2, r_1^2 r_3^2, \ldots, r_i^2 r_j^2, r_1^2 r_2^2 r_3^2, \ldots$.

Also, take for the values of $x$ those that are close in value to $\sqrt{N}$. Thus, we will know in advance certain factors of $R$ and likely not have much trouble in putting $R$ in the form $ay^2$, where $a$ is square-free. According to Kraitchik the factors of $R$ will fall into three categories:

(i) small factors of about the same size as the $r_i$, but which were not included among the $r_i$-values;
(ii) factors of value about $\sqrt[4]{N}$;
(iii) large factors.

The factors in the first category can be added to the list of possible $r_i$-values; those of the second category can be used to search for residues of $x$ such that $\pm(x^2 - N)$ is divisible by the squares of those factors; and those of the third category can be used for finding values of $x$ such that $\pm(x^2 - N)$ is divisible by these factors, but not their squares.

He provides the following example. Consider $N = 535 \cdot 2^{30} + 1$. One finds $N = 1054929^2 - 2 \cdot 2909 \cdot 9620^2$; one then finds $N = 327679^2 + 2 \cdot 2909 \cdot 8960^2$. (Note that $1054924 - 327679 = 2909 \cdot 250$.) Since both $-2 \cdot 2909$ and $2 \cdot 2909$ are quadratic residues of $N$, their product must be, and since this is $-5818^2$, we see that $-1$ is a quadratic residue of $N$. One finds further that

$$\begin{aligned} N &= 718721^2 + 41 \cdot 353 \cdot 2000^2, \\ N &= 714485^2 + 2 \cdot 13 \cdot 37 \cdot 353 \cdot 434^2, \\ N &= 757671^2 + 13 \cdot 37 \cdot 41 \cdot 140^2. \end{aligned}$$

(Note $718721 - 714485 = 12 \cdot 353$, $757671 - 718721 = 41 \cdot 950$.) Thus $-41 \cdot 353$, $-2 \cdot 13 \cdot 37 \cdot 353$, $-13 \cdot 37 \cdot 41$ are each quadratic residues of $N$. Their product is $-2$ times a perfect square; hence $-2$ (or, in this case, 2) is also a quadratic residue of $N$.

Kraitchik became quite skilled at this sort of trial and error process for finding quadratic residues. On seeing these ideas, one is very much reminded of the work of Seelhoff [**166**]. This is not too surprising when it is pointed out that a French translation of [**166**] appeared in 1912 in *Sphinx-Oedipe.*

Notice that, although Kraitchik was completely familiar with Legendre's idea of using continued fractions to find quadratic residues (see §8), he did not, in general, advocate using this method. This is because he could not control the finding of a second factorization of some $Q_i$ having some of the same prime factors as another $Q_j$ that he had already factored. Given that a prime $p$ divides some $Q_j$, it seems to be rather difficult to predict another place in the continued fraction where $p$ divides the corresponding $Q_i$.

Kraitchik seems to have had at least three reasons for wanting to find these quadratic residues. First, if $p$ is an odd prime such that $\left(\frac{N}{p}\right) = 1$, then if $(-1)^{(p-1)/2}p$ is a quadratic residue of $N$, he showed in [**55**, pp. 150–153] that

$$a^2 - b^2 \equiv N \pmod{p} \tag{13.1}$$

has exactly $(p+1)/4$ solutions for $a$ modulo $p$ when $p \equiv -1 \pmod 4$, and either $(p-1)/4$ or $(p+3)/4$ solutions (depending on whether $\left(\frac{N}{p}\right)_4 = 1$ or $-1$) when $p \equiv 1 \pmod 4$. This is a more precise version of Cole's observation in [**19**], and, of course, it is very useful to use such a $p$ as an exclusion modulus when we want to set up our sieving algorithm for solving $a^2 - b^2 = N$, as we have cut in half the usual number of solutions of (13.1).

Second, Kraitchik [**55**, pp. 195–208] had developed a method of factoring an integer $N$ which made use of what he called 'cycles'. Suppose we have a set of congruences $a_i x_i^2 \equiv b_i y_i^2 \pmod N$ $(i = 1, 2, \ldots, k)$. This is what Kraitchik called a cycle. If

$$\prod_{1 \le i \le k} a_i = dA^2; \quad \prod_{1 \le i \le k} b_i = dB^2,$$

$$\prod_{1 \le i \le k} x_i = X; \quad \prod_{1 \le i \le k} y_i = Y,$$

we get $(AX)^2 \equiv (BY)^2 \pmod N$ (if $\gcd(d, N) = 1$). If $AX \equiv \pm BY \pmod N$, the cycle was called *primitive*; if this were not the case, the cycle was called *derived.* Of course, a derived cycle leads to a factorization of $N$, since $N > \gcd(AX - BY, N) > 1$. Kraitchik used this idea, in connection with his means of finding quadratic residues, to factor several values of $N$. For example, let $N = 409 \cdot 2^{30} + 1$. Kraitchik always kept his examples to less than 15 digits; that way, he could use D. N. Lehmer's [**92**] factor tables up to $10^7$ in order to factor his values of $\pm(x^2 - N)$. By using his technique to find values of $x, y, a$ such that $N = x^2 \pm ay^2$, he found

$$\begin{aligned} 976169^2 &\equiv 31^2 \cdot 23^2 \cdot 7^2 \cdot 2^4 \cdot 1289, \\ 47^2 \cdot 11^2 \cdot 2^3 \cdot 7 \cdot 1289 &\equiv -647971^2, \\ 661761^2 &\equiv -29^2 \cdot 2^9 \cdot 7 \cdot 409, \\ 709823^2 &\equiv 47^2 \cdot 7^2 \cdot 2^7 \cdot 7 \cdot 23 \cdot 29, \\ 41^2 \cdot 7^2 \cdot 2^7 \cdot 7 \cdot 23 \cdot 29 &\equiv -624447^2, \\ 409 \cdot 2^{30} &\equiv -1. \end{aligned}$$

Taking the products of both sides and deleting common factors, we get

$$(2^{10} \cdot 11 \cdot 41 \cdot 976169 \cdot 661761 \cdot 709823)^2 \equiv (7 \cdot 23 \cdot 29 \cdot 31 \cdot 647971 \cdot 624447)^2 \pmod N$$

or

$$50511214193^2 \equiv 132469785291^2 \pmod N,$$

from which we get

$$N = 14621 \cdot 30036277.$$

This technique is little more than a slight variation of that of Seelhoff [**166**], and, as mentioned earlier, can be regarded as an early ancestor of modern methods like the Quadratic Sieve Algorithm and CFRAC.

In [**90**] Lehmer and Powers described a method of factorization which utilizes continued fractions to obtain cycles. From (8.3) we note that if we put $Q_n^* = (-1)^n Q_n$, we get

$$A_{n-1}^2 \equiv Q_n^* \pmod N.$$

Thus, if we find a set $\{Q_{n_1}^*, Q_{n_2}^*, \ldots, Q_{n_k}^*\}$ of some of these $Q_n^*$-values such that

$$\prod_{1 \le i \le k} Q_{n_i}^* = B^2 \quad (B \in \mathbb{Z}),$$

then putting $a_i = 1$, $x_i = A_{n_i - 1}$, $b_i = Q_{n_i}^*$, $y_i = 1$, we would get a cycle, and this might lead to a factorization of $N$. When this idea was published in 1931, it was not considered by Lehmer to be practical; indeed, his own experience with it had been most frustrating. It was not until 1970, that a practical version of this idea, developed by Morrison and Brillhart [**133**], succeeded in factoring $F_7$. Their method, now commonly referred to as CFRAC (Continued Fraction), is discussed at length in [**134**], and the central idea in it is at the heart of most modern general-purpose factoring techniques. This is the technique that ended the dominance of the number sieve in factorization.

Kraitchik's third use for quadratic residues was, unfortunately, not as scientific as the first two. He may have developed this idea from a fallacious principle of Seelhoff [**169**], which seems to have been accepted by Cole [**19**]. In Seelhoff's form, the principle seems to assert that if at least $r$ primes such that $2^r > \pi(\sqrt{N})$ can be found, which when taken with the proper sign (see discussion below) are quadratic residues of $N$, then $N$ is a prime. Now as Lehmer [**77**] rightly asserts, this principle allows us to get rid of the hardest part of attempting to construct a primality test, namely the problem of combining all the acceptable residues or sieving. No proof of this principle is offered by Seelhoff, and his example is wrong. He considers the factor $N = 204084568497$ of $2^{43} - 1$ and shows that $-1, 2, 7, 11, 17, 19, 23, 31, 43, 53, 61, 67, 83, 97, 113, 131$ are all quadratic residues of $N$. Since $2^{15} > \pi(\sqrt{N})$, $N$ must be a prime. However, Landry had found 17 years earlier that $N = 9719 \cdot 2099863$. Clearly, $-1$ is not a quadratic residue of $N$; Seelhoff must have made an arithmetic error. ($-1$ is not a prime, but the knowledge that $-1$ is a quadratic residue is used in determining other quadratic residues.)

This principle occurs again in a somewhat different guise in Kraitchik's [**56**], an entire book practically devoted to it. He bases his idea on the following (unproved) theorem: If every prime $p$ such that $\left(\frac{N}{p}\right) = 1$ is such that $p$, taken with the proper sign, is a quadratic residue of $N$, then $N$ is a prime. Although he does not say this explicitly, the proper sign is $(-1)^{(p-1)/2}$ when $p$ is odd, $-1$ when $p = 2$ and $N \equiv 3, 5 \pmod 8$, $+1$ when $p = 2$ and $N \equiv 1, 7 \pmod 8$ (see §14.) In fact, Hall [**44**] showed later that this theorem is true when we replace the conclusion with the words: then $N$ is a prime or a prime power. Of course, this is not a useful primality test, so Kraitchik simply asserts that $N$ is a prime if a sufficient number of such $p$ can be found. This number is not defined, but seems, rather, to be up to the discretion of the user as long as it is large enough. This is hardly scientific, and it was vigorously criticized by Lehmer [**77**] and Beeger [**7**]. Kraitchik's unsatisfactory response in [**57**] did not really address the theoretic aspects of his principle but instead concentrated, and this only briefly, on what he claimed was the question of practicality.

He used his principle in [**56**] to 'prove' that

$$(2^{96}+1)/(2^{32}+1), (2^{93}-1)/(17(2^{31}-1))$$

are primes (they are) and that

$$(2^{120}+1)(2^8+1)/((2^{24}+1)(2^{40}+1)), N = 4(3^{55}+1)/((3^{11}+1)(3^5+1))$$

are primes (they aren't). Indeed he devotes twenty pages of [**56**] to showing that this latter number is a prime. He finds after much labour that

$$-1, 2, 3, 5, 7, 11, 13, 17, 19, 37, 41, 47, 53, 59, 67, 71, 73, 79, 89, 101, 103, 127, 137,$$

$$139, 193, 337, 419, 421, 487, 547, 643, 677, 761, 1279, 1877, 5711$$

are all quadratic residues of $N$ and concludes that $N$ must be prime (with "moral certainty"). In fact, according to Brillhart [**12**], Riesel found that $N$ is divisible by 65967. Kraitchik, as in the case of the factor of $2^{120} + 1$ (see Lehmer [**83**]), must have made one or more simple arithmetic errors. For example, we see that $-1$ cannot be a quadratic residue of $N$.

Kraitchik was more successful when he used his criterion to provide evidence that $N$ is not a prime. He does this several times in [**56**], and when he becomes sure that the number he is testing is not a prime, he then attempts to factor it. In one interesting instance of identifying an integer to be prime, Kraitchik did turn out to be correct.

Recall that Lehmer had determined that $3^{N-1} \pmod N$ for $N = (10^{23} - 1)/9$ was not 1. According to [**56**, p. 39], he asked Kraitchik to factor $N$. Kraitchik found some quadratic residues of $N$ and then used them to find the forms of the divisors $< 10^8$ that would divide $N$. He found no factor; he then used his sieving process and still found no factor. As he points out in [**56**, pp. 47–48], this would constitute a proof of the primality of $N$ except that the large number (4367532788) of possible values for $a$ in (13.1) rendered this proof very indirect. He then obtained more quadratic residues of $N$ and this convinced him that $N$ must be a prime.

He communicated his conviction to Lehmer on September 23, 1928. Lehmer then re-evaluated $3^{N-1} \pmod N$ and again did not get 1, but he also didn't get the answer he got before. Kraitchik then attempted to evaluate $3^{N-1} \pmod N$ and also made an error. Finally, in a letter of December 25, 1928 Lehmer could assert that $N$ is a prime. The proof given in [**75**] is very simple and is a beautiful representative of Lehmer's methods.

Lehmer evaluated $3^{N-1} \pmod N$ and finally got 1; he then computed $r_1 \equiv 3^{(N-1)/11} \pmod N$ and $r_2 \equiv 3^{(N-1)/4093} \pmod N$. Since $\gcd(r_1 - 1, N) = \gcd(r_2 - 1, N) = 1$, any prime factor of $N$ must have the form $11 \cdot 23 \cdot 4093n + 1 = 11390819n + 1$. Thus, the smallest possible prime factor of $N$ must exceed $2 \cdot 11390819 = 22781638$.

If we try to express $N = a^2 - b^2$, then $a = 11390819^2 n + 115222895547343$. If we restrict $a$ modulo 12 and 25, the least possible value for $a$ is 5435003952668544. But $a < \frac{1}{2}(m + N/m)$ when $m > 22781638$; hence, $a < 243861122499491 < 5435003952668544$ and $N$ must be a prime.

## 14. A modern version of Kraitchik's principle

A few years after the appearance of [**56**], Hall [**44**] attempted to put Kraitchik's principle on a more solid mathematical footing. He first defined what he called apparent residues and nonresidues of an integer $N$. If $p$ is an odd prime and $p' = (-1)^{(p-1)/2}p$, then $p'$ is an apparent residue or nonresidue of $N$ according as the value of the Legendre symbol $\left(\frac{N}{p}\right) = +1$ or $-1$, respectively. Also, $-1$ is an apparent residue or nonresidue of $N$ when the Jacobi symbol $(\frac{-1}{N}) = 1$ or $-1$, and the apparent residue or nonresidue character of 2 is defined similarly.

He then went on to consider integers $L_p$ which he defined as the least nonsquare positive integer congruent to 1 modulo 8, such that $(\frac{L_p}{q}) = 1$ for all odd primes $q \leq p$. Curiously, Kraitchik had considered these numbers previously in [**54**, pp. 41–46], where he tabulated them up to $L_{47}$ by making use of his moveable paper strips method of sieving. This table was later extended by Lehmer in [**74, 86**]; also, in [**86**] Lehmer introduced the term *pseudosquare* for any such $L_p$. In Table 1 below we give all the pseudosquares that are currently known.

The main theorem of [**44**] is the following:

THEOREM 14.1. *If all the factors of $N$ are less than $L_p$ and if $-1, 2, \dots,$ $(-1)^{(p-1)/2}p$ can be divided into two classes, $A = \{a_1, a_2, \dots, a_r\}$ (the apparent residues of $N$), and $B = \{b_1, b_2, \dots, b_s\}$ (the apparent nonresidues of $N$) such that every member of $A$ is a true quadratic residue of $N$ and the product of every pair of elements from $B$ is also a true quadratic residue of $N$, then $N$ is either a prime or a prime power.*

This test was actually used by Beeger [**8**] to show that the large factor $N = 9298142299081$ of $12^{45} + 1$ is a prime. He noted that it had previously been shown that any prime divisor of $N$ must exceed $10^5$; hence, any prime divisor of $N$ must be less than $N/10^5 < L_{67}$. Further,

$$-1, 2, -3, 5, -11, 13, 17, -23, 29, -31, -43, -47, 53, -59, 61$$

are all apparent residues of $N$ and $-7, -19, 37, 41, -67$ are apparent nonresidues of $N$. By using Kraitchik's method to find quadratic residues of $N$, he was able to show that $-1, 2, 3, 5, 11, 13, 17, 23, 29, 31, 43, 47, 53, 59, 61, 7\cdot19, 7\cdot37, 7\cdot41, 7\cdot67$ are all quadratic residues of $N$; hence, $N$ must be a prime or prime power. Since $N < 10^{15}$, and $N$ is not a perfect square, $N$ is a prime.

The main difficulty with this technique is that determining the quadratic residues of $N$ is a rather slow, trial and error process. This problem can be solved by making use of an idea of Selfridge and Weinberger mentioned in [**186**]. When this is done, we get the following theorem:

THEOREM 14.2. *If*

(i) *No prime factor of an odd $N$ is $\leq B$;*
(ii) *$N/B < L_p$;*
(iii) *$p_i^{(N-1)/2} \equiv \pm 1 \pmod{N}$ for all primes $p_i \leq p$;*
(iv) *$p_j^{(N-1)/2} \equiv -1 \pmod{N}$ for some odd $p_j \leq p$ if $N \equiv 1 \pmod{8}$; or $2^{(N-1)/2} \equiv -1 \pmod{N}$ if $N \equiv 5 \pmod{8}$,*

*then $N$ is a prime or prime power.*

| $p$ | $L_p$ | Comments |
|---|---|---|
| 3 | 73 | Kraitchik |
| 5 | 241 | (1924) [**54**] |
| 7 | 1009 | Moveable Strips |
| 11 | 2641 | |
| 13 | 8089 | |
| 17 | 18001 | |
| 19 | 53881 | |
| 23 | 87481 | |
| 29 | 117049 | |
| 31 | 515761 | |
| 37 | 1083289 | |
| 41 | 3206641 | |
| 43 | 3818929 | |
| 47 | 9257329 | |
| 53 | 22000801 | Lehmer (1928) [**74**] |
| 59 | 48473881 | Bicycle chains |
| 61 | 48473881 | |
| 67 | 175244281 | Lehmer (1954) [**86**] |
| 71 | 427733329 | SWAC |
| 73 | 427733329 | |
| 79 | 898716289 | |
| 83 | 2805544681 | Lehmer, Lehmer, |
| 89 | 2805544681 | Shanks (1970) [**87**] |
| 97 | 2805544681 | DLS-127 |
| 101 | 10310263441 | |
| 103 | 23616331489 | |
| 107 | 85157610409 | |
| 109 | 85157610409 | |
| 113 | 196265095009 | |
| 127 | 196265095009 | |
| 131 | 2871842842801 | Lehmer |
| 137 | 2871842842801 | (Unpublished) |
| 139 | 2871842842801 | DLS-57 |
| 149 | 26250887023729 | |
| 151 | 26250887023729 | |
| 157 | 112434732901969 | Williams (1988) |
| 163 | 112434732901969 | (Unpublished) |
| 167 | 112434732901969 | UMSU |
| 173 | 178936222537081 | |
| 179 | 178936222537081 | |
| 181 | 696161110209049 | |
| 191 | 696161110209049 | |
| 193 | 2854909648103881 | Stephens and Williams [**175**] |
| 197 | 6450045516630769 | OASiS (1989) |
| 199 | 6450045516630769 | |
| 211 | 11641399247947921 | |
| 223 | 11641399247947921 | |

TABLE 1. Table of Pseudosquares

Notice that if $B = 1$ and $N$ is a prime, there must exist some odd $q \leq p$ such that $\left(\frac{N}{q}\right) = -1$ when $N \equiv 1 \pmod 8$. If $N \equiv 5 \pmod 8$, then $\left(\frac{2}{N}\right) = -1$. Thus, both conditions (iii) and (iv) must hold when $N$ is a prime and $B = 1$.

The next problem we encounter on using this test is the growth rate of $L_p$. Clearly, if we could show that $L_p$ grows rapidly, we would have an efficient primality test. In fact, Bach [**5**] has shown that if $G$ is a nontrivial subgroup of $R$, the group of reduced residues modulo $m$, such that $n \in G$ for all $0 < n < x$, then $x < 2(\log m)^2$. (The value 2 can be replaced by a somewhat smaller constant for sufficiently large values of $m$.) If we put $m \equiv 1 \pmod 8$ and define $\left(\frac{a}{m}\right)$ to be the Jacobi symbol, then if $G$ is the group of reduced residues of $a$ modulo $m$ where $\left(\frac{a}{m}\right) = 1$, $G$ is a subgroup of $R$. Also, if $m$ is not a perfect square, then $p^a \,\|\, m$ with $a$ odd for some odd prime $p$. If we let $t$ be some integer such that $\left(\frac{t}{p}\right) = -1$, and put

$$\begin{aligned} b &\equiv t \pmod{p^a}, \\ b &\equiv 1 \pmod{m/p^\alpha}, \end{aligned}$$

then $\left(\frac{b}{m}\right) = \left(\frac{b}{p^\alpha}\right) = \left(\frac{b}{p}\right) = \left(\frac{t}{p}\right) = -1$, $\gcd(b, m) = 1$ and $1 < b < m$. Hence, $b$ is a reduced residue which is not in $G$, and therefore $G$ is a proper subgroup of $R$.

If we put $m = L_p$, then $\left(\frac{n}{m}\right) = 1$ for all $1 \leq n \leq p$ and we get $p < 2(\log L_p)^2$. It follows that

$$L_p > e^{\sqrt{p/2}}. \tag{14.1}$$

Unfortunately, Bach's result is conditional on the truth of the Extended Riemann Hypothesis (ERH), a hypothesis which has not yet been proved; indeed, there are some who believe that it is false. Certainly, the values of $L_p$ computed so far satisfy (14.1). If the ERH is ever proved, or the restriction of the ERH could be removed from Bach's theorem, we would have a primality test which satisfies all the desiderata of §2.

## 15. Conclusion

We have concluded this paper in much the same way as we began it, by discussing primality tests. We should in this connection mention that just at the beginning of the development of computers, the prime character of all the Mersenne numbers $M_p$ for $p \leq 257$ had been determined without the use of a computer. This achievement was due greatly to the immense efforts of H.S. Uhler [**180, 181, 182, 183, 184**], who (correctly) showed that $M_{157}$, $M_{167}$, $M_{199}$, $M_{227}$ and $M_{193}$ are all composite by using the Lucas-Lehmer test. Briefly put, Uhler's [**179, 180**] modification to the test technique of Lehmer consisted of replacing the division by $M_p$ by the less time-consuming process of multiplication by an approximation to $1/M_p$.

The largest integer ever proved prime without the use of a computer is the 44-digit $(2^{148}+1)/17$. This was done by Ferrier [**29**] in 1952 by using essentially the same technique that Lehmer used to prove $(10^{23} - 1)/9$ a prime.

We realize that there are many whose names we have not mentioned in this history and many other developments that we have left undescribed. In spite of the length of the paper, we have not made any attempt at completeness — that would require a book. Rather, we have attempted only to outline the main developments of our subject. It is our hope that the reader has gained some appreciation for all the work that was done before computers appeared on the scene and now understands why the introduction of these machines caused such a sudden acceleration in the further development of Computational Number Theory. Indeed, this is one of the few papers on the subject that will not soon be out of date.

One problem that is of great importance to us is the determination of the growth rate of $L_p$. This, naturally, can be approached in several directions. One of us (HCW) is pursuing this through further computation of the $L_p$-values. This will require the construction of another sieve device which has recently been described by Patterson [**136, 137**]. This machine is planned to be able to sieve through the integers in order to find special numbers like pseudosquares at the rate of $5.38 \times 10^{11}$ per second. We recognize on saying this that one of us (at least) is promising to build a new machine. Perhaps, in view of several of our themes in this paper, it is fitting to close with the French proverb: Plus ça change, plus c'est la même chose.

## 16. Acknowledgements

The authors would like to thank Richard Mollin, Bruce Reznick and Michael Rosen for helping them to obtain various obscure library materials. Thanks are also due to Brown University for permission to use its excellent mathematics collection. We are pleased to acknowledge assistance and suggestions we received from Eric Bach, John Brillhart, Hendrik W. Lenstra, Jr. and Andrew Odlyzko. François Morain was extremely helpful in obtaining certain bibliographic information and, especially, in locating information about Carissan and his wonderful sieve. We are most grateful to Emma Lehmer for making Dick's journals, papers, etc. available to us and for reviewing a preliminary version of this paper. Finally, we thank the referee for a careful reading and useful suggestions.

## References

1. L. M. Adleman and M.-D. Huang, *Primality Testing and Abelian Varieties over Finite Fields*, Lecture Notes in Mathematics, vol. 1512, Springer-Verlag, 1992.
2. Anonymous, *Les appareils à calculs exacts et instantanés pour simplifier la multiplication et la division, inventés par M. Henri Genaille, et perfectionnés par M. Edouard Lucas*, Nouvelles Annales de Mathématiques (3) **4** (1885), 516–519.
3. A. O. L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), 29–68.
4. H. P. Babbage, *Babbage's Calculating Engines*, Spon & Company, London, 1889. Reprinted by Tomash Publishers, Los Angeles, 1982.

5. Eric Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), 355–380.
6. P. T. Bateman, J. L. Selfridge and S. S. Wagstaff, Jr., *The new Mersenne conjecture*, Amer. Math. Monthly **96** (1989), 125–128.
7. N. G. W. H. Beeger, *Sur la decomposition de grands nombres*, Nieuw Archief voor Wiskunde (2) **16** (1929/30), 37–42.
8. N. G. W. H. Beeger, *Note sur la factorisation de quelques grands nombres*, Institut Grand-Ducal de Luxembourg, Sect. d. Sc. nat. phys. math. Archives **16** (1946), 93–95.
9. E. T. Bell, *Mathematics: Queen and Servant of Science*, McGraw-Hill, NY, 1951, p. 228.
10. W. Bosma and M.-P. van der Hulst, *Primality Proving with Cyclotomy*, University of Amsterdam, 1990.
11. D. M. Bressoud, *Factorization and Primality Testing*, Springer-Verlag, New York, 1989.
12. J. Brillhart, *Fermat's factoring method and its variants*, Cong. Numerantium **32** (1981), 29–48.
13. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ Up to High Powers*, vol. 22 of Contemporary Mathematics, American Mathematical Society, 1988, 2nd Edition.
14. H. Brocard, *Question 528*, Mathesis **7** (1887), 73–75.
15. J. Brown, L. C. Noll, B. K. Parady, J. F. Smith, G. W. Smith, and E. S. Zarantonello, *Letter to the Editor*, Amer. Math. Monthly **97** (1990), 214.
16. E. Carissan, *Machine à resoudre les congruences*, Bulletin de la Société d'Encouragement pour l'Industrie Nationale **132** (1920), 600–607.
17. R. D. Carmichael, *On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$*, Ann. of Math. **15** (1913), 30–70.
18. A. Cauchy, *Sur les moyens d'éviter les erreurs dans les calculs numériques*, C. R. Acad. Sci. Paris **9** (1840), 789–798.
19. F. N. Cole, *On the factoring of large numbers*, Bull. Amer. Math. Soc. **10** (1903), 134–137. French translation in Sphinx-Oedipe **5** (1910), 122–124.
20. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1: Divisibility and Primality. Carnegie Institution of Washington, Publication No. 256, 1919. Reprinted by Chelsea Books, New York, 1971.
21. S. Drake, *The rule behind 'Mersenne's numbers'*, Physis-Riv. Internaz. Storia Sci. **13** (1971), 421–424.
22. J. D. Elder, *Factor Stencils*, Carnegie Institution of Washington, D.C., 1939.
23. J. Ewing, *The latest Mersenne prime*, Amer. Math. Monthly **99** (1992), 360.
24. E. Fauquembergue, *Question 266*, L'Intermédiaire des Mathématiciens **1** (1894), 148.
25. E. Fauquembergue, *Vérification des nombres de Mersenne*, Sphinx-Oedipe **7** (1912), 20–23.
26. E. Fauquembergue, *Réponse*, L'Intermédiaire des Mathématiciens **24** (1917), 33.
27. E. Fauquembergue, *Nombres de Mersenne*, Sphinx-Oedipe **15** (1920), 17–18.
28. P. Fermat, *Fragment d'une lettre de Fermat*, Oeuvres de Fermat **2** (1894), 256–258.
29. A. Ferrier, *The determination of a large prime*, Math. Tables and other Aids to Computation **6** (1952), 256.
30. C. F. Gauss, *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig, 1801. English translation by A. A. Clarke, Springer-Verlag, New York, 1986.
31. H. Genaille, *Calculateur ou table de multiplication*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **20** (1891), I partie, 159.
32. H. Genaille, *Piano arithmétique pour la vérification des grands nombres premiers*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **20** (1891), I partie, 159.
33. A. Genocchi, *Intorno ad alcune forme di numeri primi*, Annali Mat. Pura Appl. (2) **2** (1868/69), 256–267.
34. A. Genocchi, *Intorno a tre problemi aritmetici*, Atti della Reale Accademia delle Scienze di Torino **11** (1876), 811–829.
35. A. Gérardin, *Le Père Theophile Pepin S.J.*, Sphinx-Oedipe **5**, 1$^{\text{er}}$ trimestre (1910), 1–13.
36. A. Gérardin, *Question 278*, Sphinx-Oedipe **6** (1911), 70.

37. A. Gérardin, *Question 335*, Sphinx-Oedipe **7** (1912), 47–48. Also see p. 31.
38. A. Gérardin, *F. Proth*, Sphinx-Oedipe **7** (1912), 50–51.
39. A. Gérardin, *Réponse 335*, Sphinx-Oedipe **7** (1912), 61–64.
40. A. Gérardin, *Rapport sur diverses méthodes de solutions employées en théorie pour la décomposition des nombres en facteurs*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **41** (1912), II partie, 54–57.
41. A. Gérardin, *Dernière heure*, Sphinx-Oedipe **9** (1914), 85.
42. A. Gérardin, *Nombres de Mersenne*, Sphinx-Oedipe **9** (1914), 103–108.
43. A. Gérardin, *Machine à congruences (Modèle 1937)*, 70$^{\text{e}}$ Congrès des Sociétés Savantes de Paris et des Départements, Section des Sciences, Gauthier-Villars, Paris, 1937, p. 14; II, p. 37.
44. M. Hall, *Quadratic residues in factorization*, Bull. Amer. Math. Soc. **39** (1933), 758–763.
45. D. Harkin, *On the mathematical work of François-Édouard-Anatole Lucas*, Enseign. Math. **3** (1957), 276–288.
46. Ch. Henry, *Sur divers points de la théorie des nombres. Remarques historiques*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **9** (1880), 201–207.
47. M. Heyworth, *A conjecture on Mersenne's conjecture*, New Zealand Math. Mag. **19** (1982), 147–151.
48. O. Hoppe, *The primality of* $(10^{19} - 1)/9$, Proc. London Math. Soc. (2) **17** (1918), xix.
49. V. G. Imchenetzki and V. Bouniakowsky, *Sur un nouveau nombre premier, annoncé par le père Pervouchine*, Bull. Acad. Imp. Sci. St. Petersbourg **31** (1887), 532–533. Also in Mélanges Mathématiques et Astronomiques tirés du Bulletin de l'Académie Imperiale des Sciences de St. Petersbourg **6** (1883), 553–554.
50. R. B. Killgrove and K. E. Ralston, *On a conjecture concerning the primes*, Math. Comp. **13** (1959), 121–122.
51. M. Kraitchik, *Réponse 278*, Sphinx-Oedipe **6** (1911), 95.
52. M. Kraitchik, *Sur l'équation $x^2 - y^2 = N$*, Sphinx-Oedipe **7** (1912), 23–29.
53. M. Kraitchik, *Théorie des Nombres*, Gauthier-Villars, Paris, 1922.
54. M. Kraitchik, *Recherches sur la Théorie des Nombres*, Gauthier-Villars, Paris, 1924.
55. M. Kraitchik, *Théorie des Nombres*, T. II, Gauthier-Villars, Paris, 1926.
56. M. Kraitchik, *Recherches sur la Théorie des Nombres*, T. II, Gauthier-Villars, Paris, 1929.
57. M. Kraitchik, *Factorisation des grands nombres*, Sphinx **1** (1931), 35–37.
58. M. Kraitchik, *Introduction à la Théorie des Nombres*, Gauthier-Villars, Paris, 1952.
59. M. Kraitchik, *On the factorization of* $2^n \pm 1$, Scripta. Math. **18** (1952), 39–52.
60. G. Lamé, *Note sur la limite du nombre des divisions dans la recherche du plus grand commun diviseur entre deux nombres entiers*, C. R. Acad. Sci. Paris **19** (1844), 867–870.
61. F. Landry, *Procédés Nouveaux pour Démontrer que le Nombre 2147483647 est Premier*, Librairie Hachette, Paris, 1859.
62. F. Landry, *Aux Mathématiciens de Toutes les Parties du Monde. Communication sur la Décomposition des Nombres en Leurs Facteurs Simples*, Librairie Hachette, Paris, 1867.
63. F. Landry, *Decompositions des Nombres $2^n \pm 1$ en Leurs Facteurs Premiers de $n = 1$ à $n = 64$ (Moins Quatre)*, Librairie Hachette, Paris, 1869.
64. F. Landry, *Letter to Charles Henry*, Bollettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche **13** (1880), 469–470.
65. F. Landry, *Méthode de décomposition des nombres en facteurs premiers*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **9** (1880), 185–189.
66. F. W. Lawrence, *Factorisation of numbers*, Messenger of Math. **24** (1894/95), 100–109.
67. F. W. Lawrence, *Factorisation of numbers*, Quart. J. Pure Appl. Math. **28** (1896), 285–311. French translation in Sphinx-Oedipe 5 (1910), 98–121.
68. F. W. Lawrence, *Determination of certain primes*, Proc. Lond. Math. Soc. **28** (1896/97), 465–475.
69. E. Léger, *Note sur le partage d'une droite en moyenne et extrême, et sur un problème d'arithmétique*, Corresp. Math. Phys. **9** (1837), 483–485.
70. D. H. Lehmer, *A cross-division process and its application to the extraction of roots*,

Amer. Math. Monthly **33** (1926), 198–206.

71. D. H. Lehmer, *Note on the Mersenne number* $2^{139} - 1$, Bull. Amer. Math. Soc. **32** (1926), 522.
72. D. H. Lehmer, *Tests for primality by the converse of Fermat's theorem*, Bull. Amer. Math. Soc. **33** (1927), 327–340.
73. D. H. Lehmer, *A further note on the converse of Fermat's theorem*, Bull. Amer. Math. Soc. **34** (1928), 54–56.
74. D. H. Lehmer, *The mechanical combination of linear forms*, Amer. Math. Monthly **35** (1928), 114–121.
75. D. H. Lehmer, *On the number* $(10^{23} - 1)/9$, Bull. Amer. Math. Soc. **35** (1929), 349–350.
76. D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. **31** (1930), 419–448.
77. D. H. Lehmer, *A fallacious principle in the theory of numbers*, Bull. Amer. Math. Soc. **36** (1930), 847–850.
78. D. H. Lehmer, *Note on Mersenne numbers*, Bull. Amer. Math. Soc. **38** (1932), 383–384.
79. D. H. Lehmer, *A photo-electric number sieve*, Amer. Math. Monthly **40** (1933), 401–406.
80. D. H. Lehmer, *Some new factorizations of* $2^n \pm 1$, Bull. Amer. Math. Soc. **39** (1933), 105–108.
81. D. H. Lehmer, *A machine for combining sets of linear congruences*, Math. Annalen **109** (1934), 661–667.
82. D. H. Lehmer, *On Lucas's test for the primality of Mersenne's numbers*, J. Lond. Math. Soc. **10** (1935), 162–165.
83. D. H. Lehmer, *Sur les essais directs de primalité*, Sphinx **8** (1938), 87–88.
84. D. H. Lehmer, *Guide to Tables in the Theory of Numbers*, National Research Council, Washington, D.C., 1941.
85. D. H. Lehmer, *On the factors of* $2^n \pm 1$, Bull. Amer. Math. Soc. **53** (1947), 164–167.
86. D. H. Lehmer, *A sieve problem on "pseudo-squares"*, Math. Tables and Other Aids to Computation **8** (1954), 241–242.
87. D. H. Lehmer, E. Lehmer and D. Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. **24** (1970), 433–451.
88. D. H. Lehmer, *A history of the sieve process*, in *A History of Computing in the Twentieth Century* (N. Metropolis, J. Howlett and G.-C. Rota, eds.), Academic Press, New York, 1980, pp. 445–456.
89. D. H. Lehmer, *Factorization then and now*, Computers in Mathematics, Lecture Notes in Pure and Applied Mathematics, vol. 125, Marcel Dekker, New York, 1990, 311–320.
90. D. H. Lehmer and R. E. Powers, *On factoring large numbers*, Bull. Amer. Math. Soc. **37** (1931), 770–776.
91. D. N. Lehmer, *A new short method of multiplication*, Science **16** (1902), 71–74.
92. D. N. Lehmer, *Factor Table for the First Ten Millions containing the Smallest Factor of Every Number Not Divisible by 2, 3, 5, or 7 between 0 and 10017000.* Carnegie Institute Publication 105, Washington, D.C., 1909.
93. D. N. Lehmer, *On the multiplication of large numbers*, Amer. Math. Monthly **30** (1923), 67–68.
94. D. N. Lehmer, *Factor Stencils*, Carnegie Institution of Washington, D.C., 1929.
95. D. N. Lehmer, *On the factorization of large numbers*, University of California Chronicle **32** (1930), 326–341.
96. D. N. Lehmer, *Hunting big game in the theory of numbers*, Scripta Mathematica **1** (1932/33), 229–235.
97. E. Lehmer, *On the quartic character of some quadratic units*, J. Reine Angew. Math. **268/269** (1974), 294–301.
98. A. K. Lenstra and M. S. Manasse, *Factoring by electronic mail*, Advances in Cryptology, Eurocrypt '89, Lecture Notes in Computer Science, vol. 434, Springer, 1990, pp. 355–371.
99. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349.
100. W. Looff, *Über die Periodicität der Decimalbrüche*, Archiv der Mathematik und Physik **16** (1851), 54–57.

101. Ed. Lucas, *Sur la décomposition des nombres en facteurs premiers*, Nouvelles Annales de Mathématiques (2) **14** (1875), 523–525.
102. Ed. Lucas, *Note sur l'application des séries récurrentes à la recherche de la loi de distribution des nombres premiers*, C. R. Acad. Sci. Paris **82** (1876), 165–167.
103. Ed. Lucas, *Sur la théorie des nombres premiers*, Atti della Reale Accademia delle Scienze di Torino **11** (1875/76), 928–937.
104. Ed. Lucas, *Questions nouvelles d'arithmétique supérieure*, Nouvelles Annales de Math. (2) **15** (1876), 82–83.
105. Ed. Lucas, *Sur les rapports qui existent entre la théorie des nombres et le calcul intégral*, C. R. Acad. Sci. Paris **82** (1876), 1303–1305.
106. Ed. Lucas, *Sur la recherche des grands nombres premiers*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **5** (1876), 61–68.
107. Ed. Lucas, *Nouveaux théorèmes d'arithmétique supérieure*, C. R. Acad. Sci. Paris **83** (1876), 1286–1288.
108. Ed. Lucas, *Sur l'extension du théorème de Fermat généralisé, et du Canon arithmeticus*, C. R. Acad. Sci. Paris **84** (1877), 439–442.
109. Ed. Lucas, *Sur la division de la circonférence en parties égales*, C. R. Acad. Sci. Paris **85** (1877), 136–139.
110. Ed. Lucas, *Considérations nouvelles sur la théorie des nombres premiers et sur la division géométrique de la circonférence en parties égales*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **6** (1877), 159–167.
111. Ed. Lucas, *Extrait d'une lettre de M. Édouard Lucas*, Nouvelle Correspondance Mathématique **3** (1877), 315–316.
112. Ed. Lucas, *Recherches sur plusieurs ouvrages de Leonard de Pise et sur diverses questions d'arithmétique supérieure*, Bollettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche **10** (1877), 129–193, 239–293.
113. Ed. Lucas, *On the interpretation of a passage in Mersenne's works*, Messenger of Math. **7** (1878), 185–187.
114. Ed. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. Journ. Math. **1** (1878), 184–240, 289–321.
115. Ed. Lucas, *Sur la série récurrente de Fermat*, Bollettino di Bibliografia e di Storia delle Scienze Matematiche e Fisiche **11** (1878), 783–798.
116. Ed. Lucas, *Question 453*, Nouvelle Correspondance Mathématique **5** (1879), 137.
117. Ed. Lucas, *Question 454*, Nouvelle Correspondance Mathématique **5** (1879), 138–139.
118. Ed. Lucas, *Notice sur les Titres et Travaux Scientifiques de M. Édouard Lucas*, D. Jouaust, Paris, 1880.
119. Ed. Lucas, *Principi fondamentali della geometria dei tessuti*, L'Ingegneria Civile e le Arti Industriali **6** (1880), 104–111, 113–115.
120. Ed. Lucas, *Sur les nombres parfaits*, Mathesis **6** (1886), 145–146.
121. Ed. Lucas, *Sur le neuvième nombre parfait*, Mathesis **7** (1887), 45–46.
122. Ed. Lucas, *Théorie des Nombres*, Gauthier-Villars, Paris, 1891.
123. Ed. Lucas, *Récréations Mathématiques*, T. I, 2nd edition, Gauthier-Villars, Paris, 1891, pp. 235–236.
124. Ed. Lucas, *Récréations Mathématiques*, T. II, 2nd edition, Gauthier-Villars, Paris, 1893, pp. 230–235.
125. Ed. Lucas, *Le calcul et les machines à calculer*, *Récréations Mathématiques*, T. III, Gauthier-Villars, Paris, 1893, pp. 27–86.
126. Ed. Lucas, *Les principes fondamentaux de la géométrie des tissus*, Assoc. Française pour l'Avancement des Sciences. Comptes Rendus **40** (1911), 72–88.
127. D. Mahnke, *Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung*, Bibliotheca Math. **13** (1912–13), 29–61.
128. T. E. Mason, *Mechanical device for testing Mersenne numbers for primes*, Proc. Indiana Acad. Sci. (1914), 429–432.
129. Ministère du Commerce, de l'Industrie, des Postes et du Travail, *Catalogue Officiel des Collections du Conservatoire National des Arts et Métiers*, E. Bernard, Paris, 1906,

pp. 169–206.

130. F. Morain, *Distributed primality proving and the primality of* $(2^{3539}+1)/3$, Advances in Cryptology - EUROCRYPT '90, Springer-Verlag, Berlin, 1991, pp. 110–123.
131. J. C. Morehead, *Note on Fermat's numbers*, Bull. Amer. Math. Soc. **11** (1905), 543–545.
132. J. C. Morehead and A. E. Western, *Note on Fermat's numbers*, Bull. Amer. Math. Soc. **16** (1909), 1–6.
133. M. A. Morrison and J. Brillhart, *The factorization of* $F_7$, Bull. Amer. Math. Soc. **77** (1971), 264.
134. M. A. Morrison and J. Brillhart, *A method of factoring and the factorization of* $F_7$, Math. Comp. **29** (1975), 183–205.
135. M. d'Ocagne, *Vue d'ensemble sur les machines à calculer*, Bulletin des Sciences Mathématiques **46** (1922), 102–144.
136. C. Patterson, *A 538 Billion Integer per Second Sieve*, Proc. 1991 Canad. Conf. on Electrical and Computer Engineering, 1991, pp. 13.1.1-13.1.9.
137. C. Patterson, *The Derivation of a High Speed Sieve Device*, Ph. D. Thesis, Dept. of Computer Science, University of Calgary, Calgary, Canada, 1991.
138. T. Pepin, *Sur la formule* $2^{2^n}+1$, C. R. Acad. Sci. Paris **85** (1877), 329–331.
139. T. Pepin, *Sur la décomposition des grands nombres en facteurs premiers*, Atti della Accademia Pontificia dei Nuovi Lincei **43** (1889/90), 163–191.
140. T. Pepin, *Extension de la méthod d'Euler pour la décomposition des grands nombres en facteurs premiers*, Memorie della Accademia Pontificia dei Nuovi Lincei **9** (1893), 47–76.
141. T. Pepin, *Sur la decomposition des grands nombres en facteurs premiers*, Memorie della Accademia Pontificia dei Nuovi Lincei **17** (1900), 321–344.
142. T. Pepin, *Décomposition en facteurs premiers du nombre* $N = \frac{(151)^5-1}{5\cdot 150} = 104670701$ [sic], Atti della Accademia Pontificia dei Nuovi Lincei **54** (1901), 89–93.
143. H. C. Pocklington, *The determination of the exponent to which a number belongs, the practical solution of certain congruences, and the law of quadratic reciprocity*, Proc. Cambridge Phil. Soc. **16** (1910), 1–5.
144. H. C. Pocklington, *The determination of the prime or composite nature of large numbers by Fermat's theorem*, Proc. Cambridge Phil. Soc. **18** (1914–16), 29–30.
145. H. C. Pocklington, *The direct solution of the quadratic and cubic binomial congruences with prime moduli*, Proc. Cambridge Phil. Soc. **19** (1917), 57–59.
146. P. Poulet, *Réponse 278*, Sphinx-Oedipe **15** (1920), 74–75.
147. P. Poulet, *Note sur un Théorème de Proth*, Sphinx-Oedipe **15** (1920), 53–55, 97–100, 113–119.
148. R. E. Powers, *The tenth perfect number*, Amer. Math. Monthly **18** (1911), 195–197.
149. R. E. Powers, *On Mersenne's numbers*, Proc. London Math. Soc. (2) **13** (1914), xxxix.
150. V. R. Pratt, *Every prime has a succinct certificate*, SIAM J. Computing **4** (1975), 214–220.
151. F. Proth, *Énoncés de divers théorèmes sur les nombres*, C. R. Acad. Sci. Paris **83** (1876), 1288–1289.
152. F. Proth, *Mémoires présentés*, C. R. Acad. Sci. Paris **87** (1878), 374.
153. F. Proth, *Correspondance*, Nouvelle Correspondance Mathématique **4** (1878), 210–211.
154. F. Proth, *Sur la série des nombres premiers*, Nouvelle Correspondance Mathématique **4** (1878), 236–240.
155. F. Proth, *Lettres*, Sphinx-Oedipe **6** (1911), 36–37, 151–156.
156. M. O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), 128–138.
157. A. E. Raik, *Ural'ski matematik Ivan Mikheevich Pervoushin*, Istoriko-Matematicheskie Issledovaniya **6** (1953), 535–572.
158. C. Reid, *Perfect numbers*, Scientific American **188** (1953), 84–86.
159. K. G. Reuschle, *Mathematische Abhandlung, enthaltend: Neue zahlentheoretische Tabellen*, Stuttgart, 1856.
160. Em. Reuss, *Lettre à Lucas*, Sphinx-Oedipe **20** (1925), 6–9.
161. H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Birkhäuser, Boston, 1985.
162. R. M. Robinson, *Mersenne and Fermat numbers*, Proc. Amer. Math. Soc. **5** (1954), 842–846.
163. M. Rosen, *A proof of the Lucas-Lehmer test*, Amer. Math. Monthly **95** (1988), 855–856.
164. P. Seelhoff, *Über die vollkommenen Zahlen, insbesondere über die bis jetzt zweifelhaften Fälle* $2^{40}(2^{41}-1), 2^{46}(2^{47}-1), 2^{52}(2^{53}-1)$, Archiv der Mathematik und Physik **2** (1885), 327–329.
165. P. Seelhoff, *Notes mathématiques 6*, Mathesis **6** (1886), 100–101.
166. P. Seelhoff, *Die Auflösung grosser Zahlen in ihre Factoren*, Zeitschrift für Mathematik und Physik **31** (1886), 166–172. French translation in Sphinx-Oedipe **7** (1912), 84–88.
167. P. Seelhoff, *Die Theilbarkeit des Binoms* $2^{2^n}+1$, Zeitschrift für Mathematik und Physik **31** (1886), 172–174.
168. P. Seelhoff, *Die neunte vollkommene Zahl*, Zeitschrift für Mathematik und Physik **31** (1886), 174–178.
169. P. Seelhoff, *Ein neues Kennzeichen für die Primzahlen*, Zeitschrift für Mathematik und Physik **31** (1886), 306–310.
170. P. Seelhoff, *Zur Analyse sehr grosser Zahlen*, Archiv der Mathematik und Physik **3** (1886), 325–329.
171. H. Siebeck, *Die recurrenten Reihen vom Standpuncte der Zahlentheorie aus betrachtet*, J. Reine Angew. Math. **33** (1846), 71–76.
172. R. D. Silverman, *The multiple polynomial quadratic sieve*, Math. Comp. **48** (1987), 329–339.
173. R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), 84–85. Erratum **7** (1978), 118.
174. A. Statuti, *Cenno necrologico del Rev. Prof. P. Teofilo Pepin*, Atti della Accademia Pontificia dei Nuovi Lincei **58** (1904–05), 210–215.
175. A. J. Stephens and H. C. Williams, *An open architecture number sieve*, London Math. Soc. Lecture Note Series **154** (1990), 38–75.
176. Doron D. Swade, *Redeeming Charles Babbage's Mechanical Computer*, Scientific American **268** (2) (February 1993), 86–91.
177. P. Tannery, *Question 660*, L'Intermédiaire des Mathématiciens **2** (1895), 317.
178. P. Tannery, *Réponse*, L'Intermédiaire des Mathématiciens **5** (1898), 166.
179. H. S. Uhler, *Multiplication of large numbers*, Amer. Math. Monthly **28** (1921), 447–448.
180. H. S. Uhler, *First proof that the Mersenne number* $M_{157}$ *is composite*, Proc. Nat. Acad. Sci. **30** (1944), 314–316.
181. H. S. Uhler, *Note on the Mersenne numbers* $M_{152}$ *and* $M_{167}$, Bull. Amer. Math. Soc. **52** (1946), 178.
182. H. S. Uhler, *On Mersenne's number* $M_{199}$ *and Lucas's sequences*, Bull. Amer. Math. Soc. **53** (1947), 163–164.
183. H. S. Uhler, *On Mersenne's number* $M_{227}$ *and cognate data*, Bull. Amer. Math. Soc. **54** (1948), 378–380.
184. H. S. Uhler, *On all of Mersenne's numbers particularly* $M_{193}$, Proc. Nat. Acad. Sci. **34** (1948), 102–103.
185. G. Vacca, *Sui manoscritti inediti di Leibniz*, Boll. Bib. Storia Sc. Mat. **2** (1899), 113–116.
186. H. C. Williams, *Primality testing on a computer*, Ars Combinatoria **5** (1978), 127–185.
187. H. C. Williams, *How was* $F_6$ *factored?*, Math. Comp. **61** (1993), 463–474.

Department of Computer Science, University of Manitoba, Winnipeg, Manitoba R3T 2N2, Canada

*E-mail address*: hugh_williams@csmail.cs.umanitoba.ca

Department of Computer Science, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada

*E-mail address*: shallit@graceland.uwaterloo.ca